

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-214297
 (43)Date of publication of application : 11.08.1998

(51)Int.Cl.
 G06F 17/60
 G06F 13/00
 G06F 13/00
 G06F 15/00

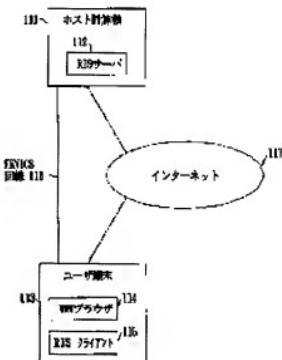
(21)Application number : 09-323626
 (22)Date of filing : 25.11.1997
 (71)Applicant : FUJITSU LTD
 (72)Inventor : OKI HIROSHI
 KAMATA SHINJI
 NAKAMURA NAOTO
 YAMAZAKI TOSHIYA
 OKADA TOSHIO

(30)Priority
 Priority number : 08318113 Priority date : 28.11.1996 Priority country : JP

(54) CLOSED-MEMBERSHIP SERVICE SYSTEM USING INTERNET, AND METHOD THEREFOR
 (57)Abstract:

PROBLEM TO BE SOLVED: To execute a safe and proper closed-membership service by using a remote install system on an internet.

SOLUTION: A remote install service(RIS) client 115 activated by a WWW browser 114 communicates a software number corresponding to an icon clicked on a home page to an RIS server 112. The RIS server 112 provides each kind of service such as software delivery, on-line shopping, communication service, and transaction service based on the information. A password or a content is enciphered and transferred on an internet 117.



(19)日本国特許庁 (JP) (12)公開特許公報 (A) (11)特許出願公開番号
 特開平10-214297
 (43)公開日 平成10年(1998)8月11日

(51)Int.Cl. ⁶	識別記号	F I	
G 06 F 17/60		G 06 F 15/21	3 3 0
13/00	3 5 1	13/00	3 5 1 H
	3 5 7		3 5 7 Z
15/00	3 3 0	15/00	3 3 0 Z

審査請求 未請求 請求項の数49 O.L. (全 56 頁)

(21)出願番号	特願平9-323626	(71)出願人	000005223 富士通株式会社 神奈川県川崎市中原区上小田中4丁目1番 1号
(22)出願日	平成9年(1997)11月25日	(72)発明者	井 宏志 神奈川県川崎市中原区上小田中4丁目1番 1号 富士通株式会社内
(31)優先権主張番号	特願平8-318113	(72)発明者	井 伸二 神奈川県川崎市中原区上小田中4丁目1番 1号 富士通株式会社内
(32)優先日	平8(1996)11月28日	(74)代理人	弁理士 大曾 義之 (外1名)
(33)優先権主張国	日本 (JP)		

最終頁に続く

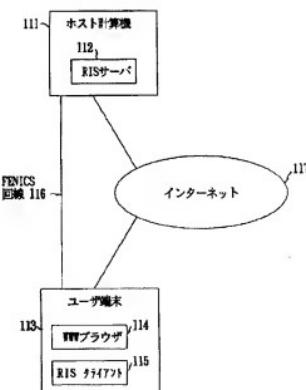
(54)【発明の名称】 インターネットを利用した会員制サービスシステムおよび方法

(57)【要約】

【課題】 インターネット上でリモートインストールシステムを利用して、安全かつ適切な会員制サービスを実現することが課題である。

【解決手段】 WWWブラウザ114により起動されたリモートインストールサービス(RIS)クライアント115は、ホームページ上でクリックされたアイコンに対応するソフトウェア番号を、RISサーバ112に通知する。RISサーバ112は、その情報を元にして、ソフトウェア配送、オンラインショッピング、通信サービス、トランザクションサービス等の各種サービスを提供する。インターネット117上で、パスワードやコンテンツは暗号化されてやり取りされる。

シス テ ム 構 成 図



【特許請求の範囲】

【請求項1】 セキュリティの確保された通信路を介して、クライアントのサインアップを行う登録手段と、前記サインアップの過程で、前記クライアントのマシン識別子に対応したキー情報を付与するキー情報付与手段と、前記キー情報を用いて、インターネット上のパスワードとソフトウェアコンテンツのうち少なくとも一方の暗号化を行う暗号化手段とを備えることを特徴とするソフトウェア配信システム。

【請求項2】 ホームページ上のアンカーファイルにより指定されるソフトウェアを、自動的にサーバからクライアントに配送するリモートインストール手段と、前記アンカーファイルがアクセスされたとき、自動的に前記リモートインストール手段を起動するブラウザ手段とを備えることを特徴とするソフトウェア配信システム。

【請求項3】 前記リモートインストール手段は、インターネットブラウザのヘルパ・アプリケーションとして登録され、前記アンカーファイルに対応する前記ホームページ上の領域がクリックされたとき、自動的に起動されることを特徴とする請求項2記載のソフトウェア配信システム。

【請求項4】 自動的にクライアントからサーバへ接続して、ホームページ上のアンカーファイルにより指定される商品またはサービスの課金処理を行く課金手段と、前記アンカーファイルがアクセスされたとき、自動的に前記課金手段を起動するブラウザ手段とを備えることを特徴とするオンラインショッピングシステム。

【請求項5】 前記課金手段は、自動的に前記サーバから前記クライアントへ情報を配送するリモートインストールシステムを含むことを特徴とする請求項4記載のオンラインショッピングシステム。

【請求項6】 前記課金手段は、インターネットブラウザのヘルパ・アプリケーションとして登録され、前記アンカーファイルに対応する前記ホームページ上の領域がクリックされたとき、自動的に起動されることを特徴とする請求項4記載のオンラインショッピングシステム。

【請求項7】 前記課金手段は、前記商品またはサービスのベンダに購入通知を送ることを特徴とする請求項4記載のオンラインショッピングシステム。

【請求項8】 ホームページ上のアンカーファイルにより指定される通信サービスの課金処理を行い、該通信サービスを利用するため必要な情報を、自動的にサーバからクライアントへ送る処理手段と、前記アンカーファイルがアクセスされたとき、自動的に前記処理手段を起動するブラウザ手段とを備えることを特徴とする通信サービスシステム。

【請求項9】 前記処理手段は、自動的に前記サーバから前記クライアントへ情報を配送するリモートインスト

ールシステムを含むことを特徴とする請求項8記載のオンラインショッピングシステム。

【請求項10】 前記処理手段は、インターネットブラウザのヘルパ・アプリケーションとして登録され、前記アンカーファイルに対応する前記ホームページ上の領域がクリックされたとき、自動的に起動されることを特徴とする請求項8記載のオンラインショッピングシステム。

【請求項11】 前記処理手段は、前記必要な情報としてパスワード情報をユーザに通知し、該ユーザは該パスワード情報を前記ブラウザ手段に入力して、前記通信サービスを利用することを特徴とする請求項8記載のオンラインショッピングシステム。

【請求項12】 前記処理手段は、前記必要な情報として前記通信サービスのURL(uniform resource locator)情報をユーザに通知し、該ユーザは該URL情報を前記ブラウザ手段に入力して、前記通信サービスを利用することを特徴とする請求項8記載のオンラインショッピングシステム。

【請求項13】 ホームページ上のアンカーファイルにより指定される通信サービスの課金処理を行い、該通信サービスのURL(uniform resource locator)を参照するブラウザを自動的に起動する処理手段と、前記アンカーファイルがアクセスされたとき、自動的に前記処理手段を起動するブラウザ手段とを備えることを特徴とする通信サービスシステム。

【請求項14】 インターネットにアクセスするブラウザ手段と、

前記ブラウザ手段により起動され、トランザクションサービスの一部の処理を行うヘラバ手段と、前記ブラウザ手段により起動され、前記ヘラバ手段と連携して、トランザクションの使用権の付与および課金に関する処理を行う処理手段とを備えることを特徴とするトランザクションサービスシステム。

【請求項15】 前記処理手段は、自動的に前記サーバから前記クライアントへ情報を配送するリモートインストールシステムを含むことを特徴とする請求項14記載のトランザクションサービスシステム。

【請求項16】 トランザクションサービスの処理を行うトランザクション手段と、

前記トランザクション手段により起動され、該トランザクション手段と連携して、トランザクションの使用権の付与および課金に関する処理を行う処理手段とを備えることを特徴とするトランザクションサービスシステム。

【請求項17】 前記処理手段は、前記トランザクションサービスの複数回の使用権を付与することを特徴とする請求項14または16記載のトランザクションサービスシステム。

【請求項18】 トランザクションサービスの処理を行うトランザクション手段と、

前記トランザクション手段により起動され、自動的にクライアントからサーバへ接続して、前記トランザクションサービスに必要なデータを取得する処理手段とを備えることを特徴とするトランザクションサービスシステム。

【請求項19】 前記処理手段は、前回のデータ更新時から所定時間経過したとき、前記サーバに接続し、前記データを取得することを特徴とする請求項18記載のトランザクションサービスシステム。

【請求項20】 クライアントから、サーバ識別子とクライアント識別子を合成して生成されたマシン識別子を受け取る受信手段と、前記マシン識別子をサーバ部とクライアント部に分解し、該サーバ部に記述されたサーバ識別子をチェックして、前記クライアントとの接続が正しいかどうかを判定する判定手段とを備えることを特徴とするサービスシステム。

【請求項21】 サーバ識別子とクライアント識別子を合成して、クライアントのマシン識別子を生成する生成手段と、前記マシン識別子を格納する格納手段と、前記マシン識別子を用いてサーバに接続する接続手段とを備えることを特徴とするサービスシステム。

【請求項22】 前記格納手段は、複数のサーバのマシン識別子を、各サーバ毎に記述した複数の初期設定ファイルを格納し、該複数の初期設定ファイルのうちの1つに、他の初期設定ファイルがあるかどうかを表す拡張情報が記述されることを特徴とする請求項21記載のサービスシステム。

【請求項23】 サーバへのログイン時に、該サーバの認証鍵に基づく電子署名機能を用いて暗号化された指定情報を送受信する通信手段と、

該指定情報を介してサーバの認証を行う認証手段とを備えることを特徴とするリモートインストールシステム。

【請求項24】 前記認証手段は、ログインの度に前記認証鍵を取得することを特徴とする請求項23記載のリモートインストールシステム。

【請求項25】 クライアント側に設けられ、インターネット上におけるサーバのアドレス情報を格納する格納手段と、前記アドレス情報を用いて、自動的に前記クライアントから前記サーバに接続する接続手段とを備えることを特徴とするリモートインストールシステム。

【請求項26】 セキュリティの確保された通信路を介して、クライアントのサインアップを行い、

前記クライアントのマシン識別子に対応したキー情報を前記クライアントに付与し、

前記キー情報を用いて、インターネット上のパスワードとソフトウェアコンテンツのうち少なくとも一方の暗号化を行うことを特徴とするソフトウェア配達方法。

【請求項27】 リモートインストールシステムをブラウザのヘルパとして登録し、

ホームページ上に前記ヘルパを起動するアンカーファイルを置き、

前記アンカーファイルがアクセスされたとき、指定されたソフトウェアを、自動的にサーバからクライアントに配送することを特徴とするソフトウェア配達方法。

【請求項28】 リモートインストールシステムをブラウザのヘルパとして登録し、

ホームページ上に前記ヘルパを起動するアンカーファイルを置き、

前記アンカーファイルがアクセスされたとき、自動的にクライアントからサーバへ接続して、指定された商品またはサービスの課金処理を行うことを特徴とするオンラインショッピング方法。

【請求項29】 リモートインストールシステムをブラウザのヘルパとして登録し、

ホームページ上に前記ヘルパを起動するアンカーファイルを置き、

20 前記アンカーファイルがアクセスされたとき、指定された通信サービスの課金処理を行い、該通信サービスを利用するために必要な情報を、自動的にサーバからクライアントへ送ることを特徴とする通信サービス方法。

【請求項30】 リモートインストールシステムをブラウザのヘルパとして登録し、

ホームページ上に前記ヘルパを起動するアンカーファイルを置き、

前記アンカーファイルがアクセスされたとき、指定された通信サービスの課金処理を行い、該通信サービスのURL (uniform resource locator) を参照するブラウザを自動的に起動することを特徴とする通信サービス方法。

【請求項31】 トランザクションサービスの一部の処理をブラウザの第1のヘルペとして登録し、

トランザクションの使用権をリモートインストールシステムに登録し、

前記リモートインストールシステムを前記ブラウザの第2のヘルペとして登録し、

前記リモートインストールシステムが前記第1のヘルペ

40 と連携して、前記トランザクションの使用権の付与および課金に関する処理を行うことを特徴とするトランザクションサービス方法。

【請求項32】 トランザクションの使用権をリモートインストールシステムに登録し、

トランザクション処理ソフトウェアから前記リモートインストールシステムを起動し、

前記リモートインストールシステムが、前記トランザクション処理ソフトウェアと連携して、前記トランザクションの使用権の付与および課金に関する処理を行うことを特徴とするトランザクションサービス方法。

【請求項3 3】 トランザクション処理ソフトウェアからリモートインストールシステムを起動し、自動的にクライアントからサーバへ接続して、トランザクションサービスに必要なデータを取得することを特徴とするトランザクションサービス方法。

【請求項3 4】 サーバ識別子とクライアント識別子を合成してマシン識別子を生成し、クライアントからサーバへ送られた前記マシン識別子をサーバ部とクライアント部に分解し、前記サーバ部に記述されたサーバ識別子をチェックして、前記クライアントとの接続が正しいかどうかを判定することを特徴とするサービス方法。

【請求項3 5】 サーバへのログイン時に、該サーバの認証鍵に基づく電子署名機能を用いて暗号化された指定情報を送りし、

該指定情報を介してサーバの認証を行うことを特徴とするリモートインストール方法。

【請求項3 6】 インターネット上におけるサーバのアドレス情報をクライアントに格納し、

前記アドレス情報を用いて、自動的に前記クライアントから前記サーバへ接続することを特徴とするリモートインストール方法。

【請求項3 7】 コンピュータのためのプログラムを記録した記録媒体であって、

セキュリティの確保された通信路を介して、クライアントのサインアップを行う機能と、

前記クライアントのマシン識別子に対応したキー情報を受信する機能と、

前記キー情報を用いて、インターネット上のパスワードを暗号化し、暗号化されたパスワードを送信する機能とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項3 8】 コンピュータのためのプログラムを記録した記録媒体であって、

セキュリティの確保された通信路を介して、クライアントからのサインアップを受け付ける機能と、

前記クライアントのマシン識別子に対応したキー情報を前記クライアントに付与する機能と、

前記キー情報を用いて、ソフトウェアコンテンツを暗号化し、暗号化されたソフトウェアコンテンツを前記クライアントに送信する機能とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項3 9】 コンピュータのためのプログラムを記録した記録媒体であって、

ホームページ上のアンカーファイルにより指定されるソフトウェアを、自動的にサーバからクライアントに配達するリモートインストール機能と、

前記アンカーファイルがアクセスされたとき、ブラウザに組み込まれた前記リモートインストール機能を自動的

に起動する機能とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項4 0】 コンピュータのためのプログラムを記録した記録媒体であって、

自動的にクライアントからサーバへ接続して、ホームページ上のアンカーファイルにより指定される商品またはサービスの課金を依頼する処理機能と、

前記アンカーファイルがアクセスされたとき、ブラウザに組み込まれた前記処理機能を自動的に起動する機能とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項4 1】 コンピュータのためのプログラムを記録した記録媒体であって、

ホームページ上のアンカーファイルにより指定される通信サービスの課金をサーバに依頼し、該通信サービスを利用するために必要な情報を、自動的に該サーバから受信する処理機能と、

前記アンカーファイルがアクセスされたとき、ブラウザに組み込まれた前記処理機能を自動的に起動するブラウザ手段とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項4 2】 コンピュータのためのプログラムを記録した記録媒体であって、

ホームページ上のアンカーファイルにより指定される通信サービスの課金を依頼し、該通信サービスのURL(uniform resource locator)を参照する第1のブラウザを自動的に起動する処理機能と、

前記アンカーファイルがアクセスされたとき、第2のブラウザに組み込まれた前記処理機能を自動的に起動する機能とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項4 3】 コンピュータのためのプログラムを記録した記録媒体であって、

インターネットにアクセスするブラウザ機能により起動され、トランザクションサービスの一部の処理を行う処理機能と、

前記ブラウザ機能により起動され、前記処理機能と連携して、トランザクションの使用権の付与および課金に関する処理を行う機能とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項4 4】 コンピュータのためのプログラムを記録した記録媒体であって、

トランザクションサービスの処理を行うトランザクション機能と、

前記トランザクション機能により起動され、該トランザクション機能と連携して、トランザクションの使用権の付与および課金に関する処理を行う機能とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ

7
 ュータ読み取り可能な記録媒体。
 【請求項 4 5】 コンピュータのためのプログラムを記録した記録媒体であって、
 トランザクションサービスの処理を行うトランザクション機能と、

前記トランザクション機能により起動され、自動的にクライアントからサーバへ接続して、前記トランザクションサービスに必要なデータを取得する機能とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 4 6】 コンピュータのためのプログラムを記録した記録媒体であって、
 クライアントから、サーバ識別子とクライアント識別子を合成して生成されたマシン識別子をサーバ部とクライアント部に分解し、該サーバ部に記述されたサーバ識別子をチェックして、前記クライアントとの接続が正しいかどうかを判定する機能とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 4 7】 コンピュータのためのプログラムを記録した記録媒体であって、
 サーバ識別子とクライアント識別子を合成して、クライアントのマシン識別子を生成する機能と、
 前記マシン識別子を格納する機能と、
 前記マシン識別子を用いてサーバに接続する機能とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 4 8】 コンピュータのためのプログラムを記録した記録媒体であって、
 サーバへのログイン時に、該サーバの認証鍵に基づく電子署名機能を用いて暗号化された指定情報を送受信する機能と、
 該指定情報を介してサーバの認証を行う機能とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 4 9】 コンピュータのためのプログラムを記録した記録媒体であって、
 インターネット上におけるサーバのアドレス情報をクライアントに格納する機能と、
 前記アドレス情報を用いて、自動的に前記クライアントから前記サーバに接続する機能とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、インターネット等の通信ネットワークを利用した会員制のサービスを提供するシステムおよびその方法に関する。

【0002】

【從来の技術】 近年のパーソナルコンピュータの普及に伴い、ユーザは通信回線を介して様々なサービスを受けられるようになります。例えば、通信回線を介してソフトウェアの配達を自動的に行う従来の技術として、「リモートインストールシステムおよび方法」(特願平7-1797、特開平8-190472)がある。

【0003】 従来のリモートインストールサービスシステム(RISシステム)は、ソフトウェアの配達センターにあるホスト計算機、ユーザ端末、およびこれらを結ぶ通信回線からなる。ホスト計算機は、配達可能な複数のソフトウェアを含むソフトウェア群と、そのソフトウェア群から特定のソフトウェアを選択するときに用いるキーワードのリストを保持する第1キーテーブルおよび第2キーテーブルを格納している。

【0004】 ユーザが端末からホスト計算機にキーワードのリストを要求すると、ホスト計算機は第1キーテーブル、第2キーテーブルを順次送信して、それらに含まれるキーワードを端末の表示装置の画面に表示させる。ユーザは表示されたキーワードから希望するソフトウェアに対応するものを選び、ホスト計算機に通知する。

【0005】 ホスト計算機は通知されたキーワードに該当するいくつかのソフトウェアの名称を含むメニューを表示装置の画面に表示させ、ユーザはその中から希望するソフトウェアを選んで、ホスト計算機に通知する。そして、ホスト計算機はソフトウェア群からユーザの選んだソフトウェアのコンテンツ(ファイル)を取り出し、端末のハードディスクに設定された配達用のディレクトリに格納する。

【0006】 このとき、宅配されたソフトウェアを起動するためのアイコンが自動的に登録され、表示装置の画面上でディレクトリに対応して設けられた倉庫ウィンドウ内に表示される。例えば誰かがWINDOWSを搭載している場合は、宅配されたソフトウェアはWINDOWSのプログラムマネージャに登録される。以後、ユーザはそのアイコンをマウス等の入力装置を用いてクリックするだけで、宅配されたソフトウェアを使用することができる。

【0007】 ここで、図4から図46までを参照しながら、従来のリモートインストールシステムによるソフトウェアの宅配の動作フローを説明する。図4において、ユーザAの端末は通信用の端末ソフトのインストール時に動作環境の情報を取得し、取得した情報を設定した環境ファイル1を作成する(ステップS1)。このとき、ユーザの端末の機種や宅配に使用する格納場所(ディレクトリ)SOUKO等の、取得に時間のかかる情報、あるいは、場合によってユーザに問い合わせなければならない情報を取得する。

【0008】 格納場所SOUKOの決定にあたっては、端末はそのハードディスクに所定の容量以上の空き領域があるかどうかを調べ、空き領域があればそのルートに

宅配用のディレクトリを作成する。このときディレクトリ名等は端末が自動的に生成し、ユーザAはそれを確認する作業のみを行う。したがって、ユーザAはディレクトリ名等を入力する必要がない。

【0009】ここでは、ユーザAの機種はTOWNSであり、SOUKOのディレクトリはD:¥SOUKO（ドライブDのディレクトリSOUKO）であることが環境ファイル1に書き込まれる。ユーザAは、必要があればD:¥SOUKOを他のディレクトリに変更することもできる。

【0010】既に設定されているパーティションに所定の容量の空き領域がなければ、別のパーティションの空き領域が一番大きい場所を探して、そこに宅配用のディレクトリを作成する。具体的には、ディレクトリD:¥SOUKOが一杯になったとすると、端末が“D:¥SOUKOが一杯です。倉庫をF:¥SOUKOに変更します。よろしいですか。”等のメッセージを表示装置の画面に表示する。

【0011】ユーザAがこれを承認すると、F:¥SOUKOが新たにSOUKOのディレクトリとなる。所定の容量の空き領域がどのハードディスクにもなかったときは、“残念ながらディスク容量が足りません。ディスクを増設してください。”等のメッセージが表示される。

【0012】次に、端末ソフトの起動時（ホスト計算機へのアクセス時）に、ハードディスクやメモリの状況等のインストール後に変化した可能性のある情報を取得する（ステップS2）。ここでは、ユーザAのハードディスクがドライブDにあり、空き容量が3000Mバイトであることが環境ファイル1に書き込まれる。こうして作成された環境ファイル1の内容は、ユーザAがホスト計算機にアクセス（接続）したときに、コマンドRIS_SENDEVNによりホスト計算機に送信される（ステップS3）。

【0013】ホスト計算機は受信した情報をユーザA環境ファイル2として保持する。ユーザA環境ファイル2には、機種、ハードディスク情報ID、格納場所SOUKOのほかに、使用しているOS（オペレーティングシステム）とその格納場所が記述されている。ここでは、ユーザAの端末のOSはWINDOWSであり、その格納場所WINDOWSはD:¥WINDOWSであることがわかる。

【0014】ホスト計算機からコマンドRIS_SENDEVNに対するレスポンスとしてRIS_SENDEVN*RESP_OKを受け取ると、端末はコマンドRISKEYLISTにより第1キーリストを要求する（ステップS4）。これに応じて、ホスト計算機21は第1キーテーブル3の内容をRIS_KEYLIST*RESPとともに送り返す。ここでは、第1キーテーブル3には、キーパー号1、2、3、…に対応するキー

ワードとして、OS／基本ソフト、開発支援、ゲーム、…・が格納されている。

【0015】これらのキーワードが第1キーリストとして表示装置の画面に表示されると（ステップS5）、ユーザAはそれらの中から第1キーワードを選び端末に入力する（ステップS6）。すると、端末はユーザAの選んだ第1キーワードのキーパー号とともに、第2キーリストを要求するコマンドRIS_KEYLISTをホスト計算機に送る（ステップS7）。ここでは、ユーザAは第1キーワードとしてゲームを選択し、それに対応するキーパー号3がホスト計算機に送られる。

【0016】第2キーリストを要求されたホスト計算機は、受け取ったキーパー号に対応して第1キーテーブル3内に格納されているポイントを用いて、対応する第2キーテーブル4を求める。その内容をRIS_KEYLIST*RESPとともに送り返す。ここでは、第2キーテーブル4には、キーパー号51、52、53、…に対応するキーワードとして、RPG、アクション、パズル／クイズ、…が格納されている。

【0017】第2キーテーブル4は第1キーテーブル3内のキーワードに対応して一般に複数受けられており、その数は第1キーテーブル3内のキーワードの数と同じか、またはそれより少ない。後者の場合には、第1キーテーブル3内の2つ以上のキーワードが同じ1つの第2キーテーブル4を指すことになる。

【0018】第2キーテーブル4内のキーワードが第2キーリストとして表示装置の画面に表示されると（ステップS8）、ユーザAはそれらの中から第2キーワードを選び端末に入力する（図4-5、ステップS9）。すると、端末はユーザAの選んだ第1および第2キーワードのキーパー号とともに、第1および第2キーワードの両方に該当するソフトウェアのリストを要求するコマンドRIS_LISTをホスト計算機に送る（ステップS10）。ここでは、ユーザAは第2キーワードとしてアクションを選択し、それに対応するキーパー号52がホスト計算機に送られる。

【0019】ソフトウェアのリストを要求されたホスト計算機は、第1および第2キーワードの2つのキーパー号を持つソフトウェアをソフトウェア群の中から検索する。このとき、検索条件として第1キーワードと第2キーワードとを区別せずに、フラットに検索を行う。また、機種やOSの種別はデフォルトのキーとして扱い、これらも加味した上で検索する。これにより、例えばTOWNS以外の機種専用のソフトウェアが検索されてくることが防止される。

【0020】そして、該当するソフトウェアの名称と番号のリストをRIS_LIST*RESPとともに端末に送る。ここでは、キーパー号3と52を持つトリス、パチンコ等のソフトウェアが該当するので、それらの名称がそれぞれのソフトウェア番号5、3等とともに端

末に送られる。

【0021】ソフトウェアのリストが表示装置の画面に表示されると(ステップS11)、ユーザAはそれらの中から希望するソフトウェアを選択し、端末に入力する(ステップS12)。すると、端末はユーザAの選んだソフトウェアの番号とともに、ユーザAの環境がそのソフトウェアの動作に適するかどうかのチェックを要求するコマンドR I S _ C H K E N Vをホスト計算機に送る(ステップS13)。ここでは、ユーザAはテリスを選択し、それに対応するソフトウェア番号5がホスト計算機に送られる。

【0022】ユーザAが選択したソフトウェアの番号を受け取ったホスト計算機は、その番号に対応するソフトウェアの動作環境とユーザAの端末の環境との整合性を調べるためにチェックスク립ト5を用意し、環境チェックを行う。

【0023】このチェックはチェックスク립ト5の実行プログラムと端末の端末ソフトとの間のやりとりにより自動的に行われるので、ユーザAは環境チェックが行われていることを必ずしも意識する必要はない(ステップS14)。ユーザAに何らかの問い合わせを行う必要が生じたときにのみ、ホスト計算機がその問い合わせを行ふ。

【0024】ここでは、ユーザAが選択したテリスの動作環境として、OSがW I N D O W S、機種がT O W N S、P C 9 8等、推奨ディレクトリ(D I R)名がT E Tであることが記述されている。これに対して、ユーザA環境ファイル2には、機種がT O W N S、OSがW I N D O W Sと記述されており、両者を比較することによって機種とOSが適合していることがわかる。

【0025】次に、テリスのチェックスク립ト5を見るとユーザA側の格納場所W I N D I RにV B R J P 2 0 0 . D L Lというファイルがあるかどうかを調査するためのコマンド”S T A @ W I N D I R @ V B R J P 2 0 0 . D L L”があるので(MQ1)、ホスト計算機はこれをR I S _ C H K E N V / R E S Pとともに端末に送る。このとき、ホスト計算機はユーザA環境ファイル2を参照して、@ W I N D I R @をD: ¥ W I N D O W Sに置き換えて送る。また、ファイルV B R J P 2 0 0 . D L Lはテリスの動作に必要なファイルの1つである。

【0026】このコマンドを受け取った端末は、ドライバのディレクトリW I N D O W SにファイルV B R J P 2 0 0 . D L Lがあるかどうか調べ、その結果をA N Sとしてホスト計算機に送り返す。ここでは、該当するファイルがなかったのでA N S = O F Fが送り返される。

【0027】端末にファイルV B R J P 2 0 0 . D L Lがないことを知ったホスト計算機は、チェックスク립ト5に従って(MQ2)、“V B R J P 2 0 0をコピー

してよいか?”という問い合わせを端末に送り、この問い合わせが表示装置の画面に表示される。ユーザAは表示された問い合わせに対する回答を入力し、端末がその回答をホスト計算機に送り返す。ここでは、A N S =はいが送り返され、ホスト計算機はチェックスク립ト5に従って、リモートインストールを承認し(R I S = O K)、V B R J P 2 0 0 . D L Lのコピーを指示するフラグ2をO Nにする(MA2)。

【0028】もし、ファイルV B R J P 2 0 0 . D L Lが端末の指定されたディレクトリにあった場合はA N S = O Nが送り返されるので、その時点でR I S = O Kとなる(MA1)。

【0029】このように環境チェックを自動的に行うことにより、ユーザAの環境に適合しないソフトウェアが配送されるのを防ぐことができる。例えば、あるパッケージソフトウェアを通信回線を介して購入した後に、特定のドライバがないとそれが動作しないことを知ったような事故が未然に防止される。

【0030】R I S = O Kになるとホスト計算機は環境チェックを終了し、判定結果(J U D G E = O K)とともに、配達先のディレクトリS O U K O D I Rを端末に送る。このS O U K O D I Rは、ユーザA環境ファイルに格納されているS O U K OのディレクトリであるD: ¥ S O U K Oの下に、テリスの推奨ディレクトリであるT E Tをサブディレクトリとして付加した形式で指定される。

【0031】このとき同時に、インストールの可否(R I S)、インストールプログラム(インストーラ)のアイコン登録の有無(I C O N)、およびダウンロードの可否(D L O A D)が端末に送られる。これらのフラグR I S、I C O N、D L O A Dにより、ホスト計算機はインストール、インストーラのアイコン登録、ダウンドロードのうちのどれが可能かを端末に通知する。

【0032】インストールとはユーザAの選んだソフトウェアを端末のシステム。例えばW I N D O W Sに登録して、端末上で使用可能にすることを意味する。したがって、この場合はそのソフトウェアの実行ファイルをW I N D O W S上でアイコン登録する作業まで含む。これに対して、インストーラのアイコン登録とはインストールを実行するプログラムを端末上でアイコン登録することを意味する。

【0033】ここでは、インストールとダウンロードが許諾され(R I S = O K, D L O A D = O K)、インストーラのアイコン登録は行わない(I C O N = N C)という条件が提示される。複雑なインストールプログラムを持つソフトウェアの場合には、インストールが許諾される代わりにインストーラのアイコン登録が必要である旨が提示される。また、W I N D O W Sを搭載している端末からT O S (T O W N SのOS)用のアプリケーションを要求されたような場合には、ダウンドロードのみが

許諾される。

【0034】次に、端末の端末ソフトはインストール、インストーラのアイコン登録、ダウソードの順に優先順位をつけて、より優先順位の高いものをデフォルトとして設定し、表示装置の画面に表示する。ここでは、ホスト計算機により許諾されたインストールとダウソードのうち優先順位のより高いインストールがデフォルトとして設定され、インストール方法選択ウィンドウに表示される。

【0035】ユーザAは表示されたインストール方法を確認して、確認した旨を入力する（ステップS15）。また、ユーザAはここで表示された設定を変更することもできる。例えば、インストーラのアイコン登録を行いたいときは、「インストール方法選択ウインドウ内の「インストーラのアイコン登録」を選択して入力する。

【0036】基本的には、ユーザAは手間をかけずにできあいのインストールを行いたい場合は「システム登録」を選択し、細かいインストール設定自分で行いたい場合は「インストーラのアイコン登録」を選択し、格納場所を後で変更したい（別の機種の端末にインストールしたい）場合は「ダウソード」を選択する。「ダウソード」を選択すれば、端末の機種とは異なる機種用のソフトウェアを入手して動作するかどうか試してみることも可能になる。

【0037】次に、端末はホスト計算機から指示された宅配用のサブディレクトリD:¥SOUKO¥TETを、ハードディスク内に自動的に生成する（ステップS16）。ここでもし、端末にサブディレクトリD:¥SOUKO¥TETが既に存在している場合は、例えばD:¥SOUKO¥TET 001というサブディレクトリをつくり、これも既に存在している場合はD:¥SOUKO¥TET 002というサブディレクトリをつくる。

【0038】テトリスのファイル本体6はファイルTET1.LZH(F1)とVBRJP200.DLL(F2)とかなり、TET1.LZHは4つのファイルTETRIS.EXE、TOWNS.DRV、PC98.DRV、およびMAC.DRCを圧縮（凍結）してできている。TET1.LZHを圧縮前の状態に伸長（解凍）するとこれらの4つのファイルに分かれるが、TET1.LZHの解凍はホスト計算機から端末に配達された後に行われる。

【0039】宅配用のサブディレクトリを生成した端末は、リモートインストールの開始を依頼するコマンドRIS_INSTALLを選択したソフトウェアの番号とともにホスト計算機に送る（図4-6、ステップS17）。これを受けて、ホスト計算機は送られた番号に対応するソフトウェアのリモートインストールを開始する。リモートインストールは、ホスト計算機が作成したテトリスのインストールスクリプト7に従って、ホスト

計算機と端末の間のやりとりにより自動的に行われる（ステップS18）。

【0040】インストールスクリプト7には、まずファイルET1.LZHをユーザA側の格納場所@SOUKO@にダウソードすることを指示する記述がある。そこで、ホスト計算機は@SOUKO@をSOUKODIR=D:¥SOUKO¥TETに置き換えて、ハードディスクのサブディレクトリD:¥SOUKO¥TETにTET1.LZHをダウソードする。

【0041】端末からダウソードの完了（OK）を通知されると、次にホスト計算機は、@WINDIR@をD:¥WINDOWSに置き換えて、ハードディスクのディレクトリD:¥WINDOWSにVBRJP200.DLLをダウソードする。

【0042】端末からダウソードの完了（OK）を通知されると、次にホスト計算機は、格納場所@SOUKO@(D:¥SOUKO¥TET)にダウソードしたTET1.LZHを解凍する指示、LHA X D:¥SOUKO¥TET¥TET1.LZHを送る。これを

20 受けて、端末はTET1.LZHを前述した4つのファイルTETRIS.EXE、TOWNS.DRV、PC98.DRV、およびMAC.DRCに解凍する。これらの4つのファイルはTET1.LZHと同じサブディレクトリD:¥SOUKO¥TETに保持される。

【0043】端末から解凍の完了（OK）を通知されると、次にホスト計算機は、格納場所@SOUKO@(D:¥SOUKO¥TET)の機種@.DRVというファイルを格納場所@WINDIR@(D:¥WINDOWS)に移動させてファイル名をFONT.DRVに変更する指示、MOVE D:¥SOUKO¥TET¥TOWNS.DRV D:¥WINDOWS¥FONT.DRVを送る。

【0044】このとき、ホスト計算機はユーザA環境ファイル2を参照して、機種@をTOWNSに置き換えて送る。これを受けて、端末はサブディレクトリD:¥SOUKO¥TETのファイルTOWNS.S.DRVをディレクトリD:¥WINDOWSに移動し（ファイル移動）、FONT.DRVというファイル名に変更する（リネーム）。

40 【0045】端末からファイル移動およびリネームの完了（OK）を通知されると、次にホスト計算機は、ファイルTETRIS.EXEのアイコン登録を行う指示、ICON TETRIS.EXEを送る。これを受けて、端末はサブディレクトリD:¥SOUKO¥TETのファイルTETRIS.EXEをアイコン化して端末内に登録する。

【0046】これにより、表示装置の画面に表示された倉庫ウインドウ内に、例えばTETRIS.EXEを起動するアイコンが表示され、アイコンをクリックすればテトリスが動作を開始する。

【0047】端末からアイコン登録の完了（OK）を通知されると、ホスト計算機はRETURNを送り返してリモートインストールの終了を端末に通知し、一連のインストール作業を終了する。リモートインストールの終了を通知された端末は、ユーザAの指示に従って次のソフトウェアの選択とそのリモートインストールを行つか、あるいは処理を終了する（ステップS19）。

【0048】このようなりモートインストールシステムを利用して、ユーザにソフトウェアを販売する場合、流通するソフトウェアを管理する従来の技術として、「ソフトウェア流通システムにおける識別子記載装置および方法」（特願平7-1798、特開平8-190529）がある。

【0049】このシステムでは、ホスト計算機はそれぞれのユーザ端末に端末識別子（マシンID：MID）を発行し、端末のユーザにはマシンIDとは別のユーザ識別子（ユーザID：UID）を発行する。また、各マシンIDに対応して端末のパスワード（マシンパスワード：MP SW）を設け、各ユーザIDに対応してユーザパスワードを設ける。

【0050】ホスト計算機はこれらのマシンID、マシンパスワード、ユーザID、およびユーザパスワードを用いて、ソフトウェアの販売先である端末とユーザの情報を管理する。

【0051】ユーザに販売したソフトウェアが何らかの原因により破壊され使用不可能となった場合には、ホスト計算機は販売記録を参照して、そのソフトウェアの復旧サービスを行なう。また、販売したソフトウェアのバージョンアップのサービスも行なう。さらに、ホスト計算機は端末に与えられるマシンパスワードを動的に変更して、アクセスが行われるたびにそれをチェックすることにより、インストールしたソフトウェアが他の端末にコピーされたかどうかを監視する。

【0052】あるユーザから他のユーザに端末の譲渡があった場合には、その端末にインストールされたソフトウェアは、そのバージョンアップや復旧等のサービスを受ける権利も含めて譲り渡すことが可能となる。このような譲渡を行なえば、不正コピーの防止にも繋がるし、権利の譲渡もスムーズに行われるため、ユーザとベンダーの双方に有益に働く。

【0053】ここで、図47から図50までを参考しながら、従来のソフトウェア流通システムにおける処理のフローを説明する。図47は、ユーザIDの登録処理のフローチャートである。処理が開始されると、まずユーザは端末を流通センターのホスト計算機に接続して（ステップS21）、名前、キャッシュカードの番号、住所等の個人情報を入力する（ステップS22）。これを受けて、ホスト計算機は仮のユーザIDと仮のユーザパスワードを発行して、ユーザの登録を行う（ステップS23）。ここで、ユーザは一旦ホスト計算機との接続を

断ち、キャッシングカードが認証されるのを待つ（ステップS4）。

【0054】キャッシングカードが認証され、流通センターから正式のユーザIDと正式のユーザパスワードとが郵送されると（ステップS25）、ユーザは再び端末をホスト計算機に接続して（ステップS26）、受け取った正式のユーザIDと正式のユーザパスワードとを入力する（ステップS27）。

【0055】これにより、ホスト計算機は正式のユーザIDとユーザパスワードを記載した郵便がユーザ本人に届いたことを確認し、そのユーザを正式に登録（本登録）して処理を終了する。このとき、郵送されたユーザパスワードと共に、別のパスワードをユーザが入力して登録することもできる。

【0056】図48は、端末IDの登録処理のフローチャートである。処理が開始されると、まずユーザは端末を流通センターのホスト計算機に接続して（ステップS31）、登録されているユーザIDとユーザパスワードを入力する（ステップS32）。その後、端末がその機種や使用OS等のマシン情報を自動的にホスト計算機に送る（ステップS33）。ホスト計算機は送られたマシン情報に端末IDと端末パスワードを付加して所定の形式で記憶し、それらの端末IDと端末パスワードを端末に送る（ステップS34）。こうして、発行された端末IDと端末パスワードは端末内にも保持される。

【0057】図49は、流通センターに登録されたユーザにネットワークを介してソフトウェアを販売する処理のフローチャートである。図49において、ユーザのリクエスト等により処理が開始されると、まずユーザの端末がネットワークに接続される（ステップS41）。次に、ホスト計算機はユーザが入力したユーザIDとユーザパスワードをチェックし（ステップS42）、それらが正しくなければ（NG）、処理を終了する。

【0058】ユーザIDとユーザパスワードが正しければ（OK）、次にホスト計算機は端末内に保持された端末IDと端末パスワードとを自動的に読み取り、これらをチェックする（ステップS43）。端末IDと端末パスワードが正しくなければ（NG）、不正コピーが行われた可能性があるので不正に対応する処理（不正処理）を行う（ステップS44）。

【0059】端末IDと端末パスワードが正しければ（OK）、商品であるソフトウェアのリストを端末の画面に表示させ、ユーザに購入する商品の選択を行わせる（ステップS45）。ユーザは表示されたリストから商品を選択し、復旧サービスの要請の場合はその旨を入力する。

【0060】次に、ホスト計算機はユーザからの要求が新規商品の購入か既に販売した商品の復旧要請かを判断し（ステップS46）、復旧要請の場合はそのユーザの購入情報を参照して、該当する商品を過去に購入してい

るかどうかを調べる（ステップS47）。ユーザが購入していない商品の復旧を要請している場合は（ステップS47、NO）、復旧サービスの対象とならないので再びステップS45の処理に戻る。

【0061】ユーザが過去に購入した商品の復旧を要請している場合は（ステップS47、YES）、ホスト計算機はネットワークを介してその商品を端末に宅配し、再インストールする（ステップS49）。そして、使用契約等に基づいてユーザに課金して（ステップS50）、処理を終了する。ただし、無償で復旧サービスを行う契約が結ばれている場合は課金は行わない。

【0062】ステップS46でユーザが新規商品の購入を要請している場合は、選択された商品の販売を決定し（ステップS48）、ネットワークを介してその商品を端末に宅配してインストールする（ステップS49）。そして、商品の代金をユーザに課金して（ステップS50）、処理を終了する。

【0063】ステップS50においては、入力されたユーザIDを待つユーザに対して代金が課されるが、ユーザIDの管理はユーザに委ねられる。各ユーザはそのユーザIDを指定してユーザIDを管理する。

【0064】商品の販売契約がユーザを対象とせずに、インストールする端末に対して販売することにになっている場合は、ステップS50において端末に対して代金が課金される。この場合は、ステップS47においてその端末が該当する商品を過去に購入しているかどうかを調べ、購入していたときにのみ復旧サービスを行う。

【0065】また、端末IDについては、ホスト計算機が端末パスワードを付加し、端末が1回接続される毎にその端末の端末パスワードを自動的に書き換えて管理する。不正コピーが行われると、書き換え前の端末パスワードと共にアクセスが行われるため、その事実を認識することが可能になる。端末IDおよび端末パスワードについては、ホスト計算機がパックトレースを行うことができる。

【0066】図50は、ステップS43における端末パスワードのチェックと書き換え、およびステップS44の不正処理のフローチャートである。図50において処理が開始されると、ホスト計算機は接続された端末の端末パスワードを、その端末の前回接続時に付与した端末パスワードと比較する（ステップS51）。

【0067】それらが一致すれば、新しい端末パスワードを生成してその端末内に書き込み、ホスト計算機内にも保持しておく（ステップS52）。このとき、ホスト計算機は例えは乱数のように予想できないものを用いて、次の端末パスワードを決定する。また、書き換えられた古い端末パスワードは後で参照するために保存しておき（ステップS53）、処理を終了する。

【0068】ステップS51で2つの端末パスワードが一致しないときは、ホスト計算機は不正コピーが行われ

たと判断し、接続された端末に新しい端末IDを付与して新規に管理する（ステップS54）。そして、接続時における端末パスワードを保存されている古い端末パスワードと順次比較して、その端末パスワードによるアクセスがあった日時を求める（ステップS55）。これにより、不正コピーが行われたタイミングを特定して処理を終了する。

【0069】また、リモートインストールシステムにユーザが作成したソフトウェアを登録する先頭の技術としては、「ソフトウェア登録システムおよび方法」（特願平7-258506）がある。

【0070】図51は、このシステム内での場の構成を示している。図51のシステムにおいては、ホスト計算機の中に仮想的につくられた、クラブと呼ばれるユーザのグループが最小単位となり、ソフトウェア情報の交換の場を形成する。クラブの構成員は会員とも呼ばれる。クラブ12、13、14は同じ階層に属し、それぞれが会議室機能とリモートインストールシステム（RIS）の機能を持つている。

【0071】これらのクラブ12、13、14の上位階層には上位クラブ11がある。この例ではクラブの階層は2階層であるが、一般的には何階層でもよい。分配されるコンテンツとなるソフトウェアは、必ず、いずれかのクラブにアップロードされ、そこに登録される。例えば、ソフトウェア15がクラブ12にアップロードされると、クラブ12に最初に登録され、クラブ12はソフトウェア15のオリジナルクラブとなる。オリジナルクラブに登録されたソフトウェアを他のクラブに持つて行くには、転載という方法と移管という方法がある。

【0072】転載とは、ソフトウェアを他のクラブからも見えるようにすることを意味し、移管とは、オリジナルクラブの機能そのものを他のクラブに移すことを意味する。ソフトウェア15を希望する会員は、オリジナルクラブ12または転載先クラブ11、13のいずれかから、それをダウンロードすることができる。

【0073】基本的には、オリジナルクラブを選ぶ権利はソフトウェア15を作成した会員が持っている。しかし、作者がソフトウェア15をアップロードして、一旦公開を許可したら、それを他のクラブに転載または移管する権利はオリジナルクラブの管理者に移る。現実の運用に当たっては、アップロードした作者や各クラブの管理者の間でこれらの権利について交渉する必要があるが、コンピュータ内の仕組みとしては、それぞれの権利をあらかじめ次のように決めておく。また、作者や各管理者の義務は、契約によって例えば次のように決められる。

(1) 一般作者の権利と義務

コンテンツ（ソフトウェア）をアップロードする権利
自分のアップロードしたソフトウェアを無償でテスト充配する権利（テスト時のRISの料金が無償になる）

ソフトウェアの公開を許可する権利

自分のアップロードしたソフトウェアをサポートする義務（ソフトウェアの利用者からの質問に答えたり、エラーが発生した時の修正を行ったりする）

（2）オリジナルクラブ管理者の権利と義務

クラブ内のソフトウェアを無償でテストする権利（テスト時のソフトウェア使用料が無償になる）

ソフトウェアを公開する権利

転載先クラブに転載の許可を出す権利

クラブ内のソフトウェアをサポートする義務

上位クラブには、特別な理由がない限り、転載の許可を出す義務。

（3）転載先クラブ管理者の権利と義務

転載が許可されたソフトウェアを公開する権利

クラブ内のソフトウェアをサポートする義務

（4）上位クラブ管理者の権利

転載の許可されたソフトウェアを公開する権利

上位クラブは、基本的に下位クラブのソフトウェアを転載することができる所以、最上位のクラブの会員はすべてのソフトウェアを閲覧することができるようになる。また、転載クラブの管理者がソフトウェアの使用方法等を確実にサポートしてくれる事を条件に転載するので、ソフトウェアが閲覧可能なクラブ内で、そのサポートが必ず受けられる。

【0074】ここで、図52から図54までを参照しながら、ソフトウェア登録システムにおける作者や管理者の作業の手順について説明する。図52は、作者の作業のフローチャートである。作業が開始されると、作者は、まずソフトウェアを作成し、アップロードに必要なファイル群を用意する（ステップS61）。次に、アップロードするクラブを選択し、コマンドUPLOADによりソフトウェアをアップロードして（ステップS62）、アップロード先での自動チェックの結果を受け取る（ステップS63）。

【0075】ここでは、誤動作チェック、ウィルスチェック、著作権や商標権のチェック等が自動的に行われる。チェックの結果（ステップS64）、エラーが発生すればエラー部分を修正し、修正部分のみ再びアップロードして（ステップS65）、ステップS63以降の作業を繰り返す。

【0076】そして、自動チェックが通ったら、次にRISによりテスト宅配を行う（ステップS66）。テスト宅配では、アップロードされたソフトウェアがリモートインストール時に問題を起こさないかどうかがチェックされる（ステップS67）。テスト宅配でエラーが発生すればエラー部分を修正し、その部分のみ再びアップロードして（ステップS68）、ステップS66以降の作業を繰り返す。テスト宅配で合格したら、PUSHによりソフトウェアの公開を許可し（ステップS69）、作業を終了する。

【0077】図53は、オリジナルクラブの管理者の作業のフローチャートである。作業が開始されると、管理者は、まず作者により公開を許可されているソフトウェアをテスト宅配し（ステップS71）、問題が無いかチェックする（ステップS72）。テスト宅配で問題がなければ、コマンドPUBLISHによりソフトウェアをオリジナルクラブの会員に公開し（ステップS73）、間隔があればそれを作者に連絡して（ステップS74）、作業を終了する。

【0078】図54は、転載先クラブの管理者の作業のフローチャートである。作業が開始されると、管理者は、希望するソフトウェアがあったら、その転載許可をオリジナルクラブに依頼する（ステップS81）。依頼に対する応答を受け取り（ステップS82）、転載が許可されなければそのまま作業を終了する。コマンドPERMITにより転載が許可されれば、コマンドLINKによりそのソフトウェアを自分のクラブに転載する（ステップS83）。この時、自分のクラブで検索しやすいようにキーワードを変更しておく。

【0079】次に、転載したソフトウェアをテスト宅配し（ステップS84）、問題が無いかチェックする（ステップS85）。テスト宅配で問題がなければ、コマンドPUBLISHによりソフトウェアをクラブの会員に公開し（ステップS86）、問題があればそれをオリジナルクラブに連絡して（ステップS87）、作業を終了する。

【0080】ところで、パソコン通信で流通しているソフトウェアには、様々な種類のものがある。例えば、フリーewareと呼ばれるものは基本的に無料で配布され、シェアwareと呼ばれるものは機能制限付きで一旦無料で送付された後、所定の代金が送金されば機能限界が解除されることになっている。また、商品として販売されているものは、基本的に代金と引き換えに送付される。

【0081】配達センターがリモートインストールの機能を利用して、ソフトウェアをユーザーに販売するサービスを行う場合、このような多様な販売形態に対応して、代金を確実に受け取ることを保証する機構が必要になる。このような代金の決済に関する先駆としては、「ソフトウェア代金決済システムおよび方法」（特願平7-258507）がある。

【0082】図55は、このシステムで用いられるファイル群のアップロード処理の例を示している。シェアwareの作者は、まず本体登録ファイルとして、CFGファイル21（AAA.CFG）、説明ファイル22（AAA.TXT）、インストール関連ファイル23（ここではアイコンファイルICON.DEF）、および本体ファイル24（AAA.LZH）を自分の端末からアップロードする。

【0083】ホスト計算機は、これらのアップロード情

報をコンテンツデータベース28に登録する。ここでは、アップロードされたソフトウェア「AAAスクエジューラ」のソフトコード、名称、タイプ(TYPE)、本体ファイル名、説明ファイル名、アイコンファイル名等が管理情報として登録されている。タイプの欄のSHA REはソフトウェアの種類がシェアウェアであることを表す。コンテンツデータベース28は、例えば、ホスト計算機内または外部のディスク装置間に設けられる。

【0084】次に、作者は送金手続きファイルとして、定義ファイル25(AAAS.CFG)、CHKファイル26(AAAS.CHK)、および書換えファイル27(INI.DEF)をアップロードする。これにより、送金手続きファイルAAASのソフトコード、名称、タイプ、CHKファイル名、後処理用のファイル名等がコンテンツデータベース28に登録される。

【0085】後処理用のファイルとして、ここでは、書換えファイル27のファイル名INI.DEFが記されている。また、タイプの欄のSOKIN#RISは、ソフトウェアの種類がシェアウェアの送金手続きファイルであることを表し、AAAS.CFGの[inst type]セクションに記述された情報を対応している。

【0086】次に、図56、57、58、59を参照しながら、アップロードされたファイル群を用いたシェアウェアの送金手続きについて説明する。シェアウェア手続きにおいては、上述のリモートインストールの手続きに加えて、プロトコル上に送金フラグを設ける。そして、端末からこのフラグを立ててソフトウェアの検索を要求することにより、シェアウェア手続きを選択できるようになる。また、端末の画面に送金フラグをON/OFFするメニューを表示させる。

【0087】この例において、シェアウェア「AAAスクエジューラ」は、送金手続きの前に、機能制限付きでユーザシステムにインストールされているものとする。ユーザがこのソフトウェアを購入しようとした時は、ホスト計算機と端末の間で次のようなコマンド/レスポンスのやりとりを行う。

【0088】端末は、まずユーザ環境をホスト計算機に送信し(図56、ステップS91)、ホスト計算機はこれを受信すると応答を返す(ステップS92)。次に、ユーザがソフトウェア検索用のキーワードリストを要求すると(ステップS93)、ホスト計算機はキーワードリストを返送する(ステップS94)。

【0089】このとき、図57に示すように、端末の画面上にはオプション手続きのメニュー29が表示され、ユーザはその中から「送金」を指定し、キーワードリストの中からキーワードを選択する。これにより、送金フラグSOKINが立てられ(オンになり)、シェアウェアの検索を開始する指示がホスト計算機に送られる(図57、ステップS95)。

【0090】ホスト計算機は、指定されたキーワードで

コンテンツデータベース28を検索し、タイプがSOK INで始まるソフトウェアの名称とその送金手続きファイル(送金ソフト)のソフトコードとを返す(ステップS96)。ここでは、「AAAスクエジューラ」、「BB Bスクエジューラ」等の名称および送金ソフトのソフトコード4000、4001等が返送されている。

【0091】端末は送金ソフトのみリストアリングし、ユーザはリストアリングされた中の特定の送金ソフトを指定する(ステップS97)。ここでは、ソフトコード4000が指定されている。ホスト計算機は、ソフトコード4000の送金ソフトの条件により端末側とネゴシエーションを行う(ステップS98)。ここでは、まず、コマンドST4を用いて、ユーザシステム内に格納された初期設定ファイルAAA.INIの位置を調べるように端末に指示する。

【0092】これを受けて、端末はAAA.INIの場所を調べ、その場所はE:¥AAAという形をホスト計算機に通知する(ステップS99)。ST4というコマンドは、あらかじめ端末側に具備されているものとする。

【0093】次に、ホスト計算機はダイアログBOX30を端末の画面に表示させ、AAA.INIの位置はE:¥AAAでよいかどうかをユーザに確認する(図58、ステップS100)。ダイアログBOX30に表示されたディレクトリが正しければ、ユーザはそのディレクトリをそのまま返送し(ステップS101)、ホスト計算機は、ユーザシステムの書き換えるべきファイルのディレクトリパスはE:¥AAA¥AAA.INIと確定する。

【0094】もし、表示されたディレクトリが正しくなければ、ユーザは正しいディレクトリ名を入力する。例えばE:¥GGG¥AAA.INIをホスト計算機に返す。AAA.INIの格納場所が確定したので、ホスト計算機は、シェアウェア送金が可能であることを端末に通知する(ステップS102)。

【0095】次に、ユーザは機能制限の解除を要求する(図59、ステップS103)。これを受けて、ホスト計算機は、定義ファイル25の[inst type]セクションを参照し、代金をそのユーザの口座等から引き落とした後に、AAA.INIの書換え手順が記述されている書換えファイルINI.DEFを送付する。さらに、定義ファイルの[inst]セクションを参照して後処理のコマンドCHGINIを送り、INI.DEFの手順に従って書換えを行なうことを端末に指示する。

【0096】これを受けて、端末はダウソードされたINI.DEFを参照し、AAA.INIを書換える。これにより、シェアウェア「AAAスクエジューラ」の機能制限が解除され、ユーザシステム上で完全に動作するようになる。その後、ホスト計算機はINI.DEFを

端末から削除して、処理を終了する。

【0097】この例では、定義ファイル 25 の [inst type] のセクションにその場で制限解除を行うという機能が記されていたので、代金の引き落としと一緒にシェアウェアの機能制限を解除した。しかし、一般的パソコン通信センターと同様に、ホスト計算機が代金引き落としと一緒に登録者への電子メールの発行だけを行う構成とすることもできる。

【0098】図 60、61、62 は、このようなソフトウェア「B B B スケジューラ」の代金引き落とし手続きを示している。ただし、この手続きの前に、シェアウェア「B B B スケジューラ」は機能削除付きでユーザシステムにインストールされているものとする。ユーザがこのソフトウェアを購入しようとしたら、ホスト計算機と端末の間で次のようなコマンド/レスポンスのやりとりを行う。

【0099】端末は、まずユーザ環境をホスト計算機に送信し（図 60、ステップ S1 1 1）、ホスト計算機はこれを受信すると応答を返す（ステップ S1 1 2）。次に、ユーザがソフトウェア検索用のキーワードリストを要求すると（ステップ S1 1 3）、ホスト計算機はキーワードリストを返送する（ステップ S1 1 4）。

【0100】このとき、図 61 に示すように、端末の画面上にはオプション手続きのメニュー 2 が表示され、ユーザはその中から「送金」を指定し、キーワードリストの中からキーワードを選択する。これにより、送金フラグ SOK1 が立てられ、シェアウェアの検索を開始する指示がホスト計算機に送られる（図 61、ステップ S1 1 5）。

【0101】ホスト計算機は、指定されたキーワードでコンテンツデータベース 2 を検索し、タイプが SOK1 で始まるソフトウェアの名稱とその送金ソフトのソフトコードとを返す（ステップ S1 1 6）。端末は送金ソフトのみリストイングし、ユーザはリストイングされた中からソフトコード 4 0 0 1 の送金ソフトを指定する（ステップ S1 1 7）。

【0102】次に、ホスト計算機はメッセージ 3 1 を端末の画面に表示させ、課金してよいかどうかをユーザに確認する（図 62、ステップ S1 1 8）。このとき、ホスト計算機は、定義ファイルの [inst type] セクションを参照し、フラグ SOK1 の値をメール発行のみを表す「0 x 0 8」に変更して、端末に返送する。

【0103】ユーザは、課金されてもよければ OK を、購入しない場合は NG を選択する。ここでは、OK が選択され、登録者に対するメールの発行の依頼が端末からホスト計算機に送られる（ステップ S1 1 9）。

【0104】これを受けて、ホスト計算機は代金をそのユーザの口座等から引き落とし、「B B B スケジューラ」の登録者に代金引き落としを知らせる電子メールを送る。メールの送付先としては、定義ファイルの [ty

p e】セクションに記述された送金先 F J O K 1 を用いる。

【0105】ホスト計算機から電子メールを受け取った登録者は、電子メール等の手段により、ソフトウェアの購入者に機能制限解除の方法を連絡する。これにより、購入者は「B B B スケジューラ」のすべての機能を使用することができるようになる。

【0106】

【発明が解決しようとする課題】しかしながら、上述のような従来のリモートインストールシステムには、次のような問題がある。

【0107】販売されるソフトウェアは秘密の情報であるため、セキュリティの確保された回線を介して宅配する必要がある。したがって、あらかじめセキュリティの確保が保証されないインターネット上に適用するためには、ハッキング防止のための対策を施す必要がある。

【0108】また、インターネット上の情報探索用ソフトウェアツールである WWW ブラウザ（world wide web browser）や、リモートインストールシステムとの連携方法としては、様々な機構が考えられ、提供するサービスに応じて適した機構を構築する必要がある。

【0109】また、従来のリモートインストールシステムにおける端末のマシン ID は、ホスト計算機がただ一つしか存在しないことを前提として作成・管理されている。このため、複数のホスト計算機を R I S サーバとしてサービスを行うと、同じマシン ID を各ホスト計算機がそれぞれ異なる端末に付与する可能性がある。この場合、ホスト計算機が端末を誤って識別するという問題が生じる。

【0110】さらに、インターネット上では識別情報等も濫用される恐れがあるため、通信相手を正確に識別することが困難である。このため、第 3 者が不正に入手した識別情報をを利用して、R I S のホスト計算機になりますことができる。このような場合、ユーザがそれを見破ることができる必要がある。

【0111】本発明の課題は、インターネット上でリモートインストールシステムを利用して、安全かつ適切な会員制サービスを実現するシステムおよびその方法を提供することである。

【0112】

【課題を解決するための手段】図 1 は、本発明のサービスシステムの原理図である。図 1 のサービスシステムは、本発明の第 1、第 2、第 3、第 4、第 5、第 6、第 7、第 8、第 9、第 10、および第 11 の原理を含む。

【0113】第 1 の原理において、サービスシステムは、登録手段 8 0 、キー情報付与手段 8 1 、および暗号化手段 8 2 を備え、ソフトウェア配送サービスを提供する。登録手段 8 0 は、セキュリティの確保された通信路を介して、クライアントのサインアップを行い、キー情報付与手段 8 1 は、上記サインアップの過程で、上記ク

ライアントのマシン識別子に対応したキー情報を付与する。そして、暗号化手段 8 は、上記キー情報を用いて、インターネット上のパスワードとソフトウェアコンテンツのうち少なくとも一方の暗号化を行う。

【0114】暗号化に用いられるキー情報は、セキュリティの確保された通信路を介してやり取りされるので、盗用されることがない。こうして付与された秘密のキー情報を用いてパスワードを暗号化することで、インターネットにおいて、リモートインストールシステムへのログインシーケンスのセキュリティを高めることができる。また、このキー情報を用いてコンテンツを暗号化することで、インターネットにおいて、リモートインストールのシーケンスのセキュリティを高めることができる。

【0115】第 2 の原理において、サービスシステムは、リモートインストール手段 8 3 とブラウザ手段 8 8 を備え、ソフトウェア配達サービスを提供する。リモートインストール手段 8 3 は、ホームページ上のアンカーファイルにより指定されたソフトウェアを、自動的にサーバからクライアントに配達し、ブラウザ手段 8 8 は、上記アンカーファイルがアクセスされたとき、自動的にリモートインストール手段 8 3 を起動する。

【0116】ブラウザ手段 8 8 がリモートインストール手段 8 3 を起動することで、ユーザが指定したソフトウェアが自動的に配達される。したがって、ユーザはリモートインストール手段 8 3 を意識することなく、インターネットのホームページ上でリモートインストールサービスを利用することができます。

【0117】第 3 の原理において、サービスシステムは、課金手段 8 4 とブラウザ手段 8 8 を備え、オンラインショッピングサービスを提供する。課金手段 8 4 は、自動的にクライアントからサーバへ接続して、ホームページ上のアンカーファイルにより指定された商品またはサービスの課金処理を行い、ブラウザ手段 8 8 は、上記アンカーファイルがアクセスされたとき、自動的に課金手段 8 4 を起動する。

【0118】課金手段 8 4 としては、例えばリモートインストールシステムが用いられ、ブラウザ手段 8 8 が課金手段 8 4 を起動することで、ユーザが指定した商品またはサービスの課金が自動的に行われる。したがって、インターネット上でリモートインストールシステムを利用したオンラインショッピングサービスが実現される。

【0119】第 4 の原理において、サービスシステムは、処理手段 8 5 とブラウザ手段 8 8 を備え、通信サービスを提供する。処理手段 8 5 は、ホームページ上のアンカーファイルにより指定される通信サービスの課金処理を行い、その通信サービスを利用するため必要な情報を、自動的にサーバからクライアントへ送る。また、ブラウザ手段 8 8 は、上記アンカーファイルがアクセスされたとき、自動的に処理手段 8 5 を起動する。

【0120】処理手段 8 5 としては、例えばリモートインストールシステムが用いられ、ブラウザ手段 8 8 が処理手段 8 5 を起動することで、ユーザが指定した通信サービスの課金と、そのサービスを利用するため必要な情報の提供が自動的に行われる。したがって、インターネット上でリモートインストールシステムを利用した通信サービスが実現される。

【0121】第 5 の原理において、サービスシステムは、ヘルパ手段 8 6 、処理手段 8 7 、およびブラウザ手段 8 8 を備え、トランザクションサービスを提供する。ブラウザ手段 8 8 は、インターネットにアクセスし、ヘルパ手段 8 6 は、ブラウザ手段 8 8 により起動され、トランザクションサービスの一部の処理を行なう。また、処理手段 8 7 は、ブラウザ手段 8 8 により起動され、ヘルパ手段 8 6 と連携して、トランザクションの使用権の付与および課金に関する処理を行う。

【0122】処理手段 8 7 としては、例えばリモートインストールシステムが用いられ、ブラウザ手段 8 8 がヘルパ手段 8 6 と処理手段 8 7 を起動し、ヘルパ手段 8 6 と処理手段 8 7 が連携することで、ユーザに対するトランザクション処理の使用権の付与と課金とが自動的に行われる。したがって、インターネット上でリモートインストールシステムを利用したトランザクションサービスが実現される。

【0123】第 6 の原理において、サービスシステムは、処理手段 8 9 とトランザクション手段 9 1 を備え、トランザクションサービスを提供する。トランザクション手段 9 1 は、トランザクションサービスの処理を行い、処理手段 8 9 は、トランザクション手段 9 1 により起動され、トランザクション手段 9 1 と連携して、トランザクションの使用権の付与および課金に関する処理を行なう。

【0124】処理手段 8 9 としては、例えばリモートインストールシステムが用いられ、トランザクション手段 9 1 が処理手段 8 9 を起動し、それと連携することで、ユーザに対するトランザクション処理の使用権の付与と課金とが自動的に行われる。したがって、ブラウザを介することなく、リモートインストールシステムを利用したトランザクションサービスが実現される。

【0125】第 7 の原理において、サービスシステムは、処理手段 9 0 とトランザクション手段 9 1 を備え、トランザクションサービスを提供する。トランザクション手段 9 1 は、トランザクションサービスの処理を行い、処理手段 9 0 は、トランザクション手段 9 1 により起動され、自動的にクライアントからサーバへ接続して、上記トランザクションサービスに必要なデータを取得する。

【0126】処理手段 9 0 としては、例えばリモートインストールシステムが用いられ、トランザクション手段 9 1 が処理手段 9 0 を起動する。処理手段 9 0 はサーバ

からデータを取得してトランザクション手段91に渡し、トランザクション手段91は、そのデータを用いてトランザクションサービスの処理を行う。したがって、ブラウザを介すことなく、リモートインストールシステムを利用したトランザクションサービスが実現される。

【0127】第8の原理において、サービスシステムは、受信手段92と判定手段93を備える。受信手段92は、クライアントから、サーバ識別子とクライアント識別子を合成して生成されたマシン識別子を受け取る。そして、判定手段93は、上記マシン識別子をサーバ部とクライアント部に分解し、そのサーバ部に記述されたサーバ識別子をチェックして、上記クライアントとの接続が正しいかどうかを判定する。

【0128】クライアントがマシン識別子にサーバ識別子を混ぜて送ることで、判定手段93は、その接続要求がどのサーバに対するものかを特定することができる。そして、サーバ識別子に対応するサーバが、クライアントの正しい接続先と判定される。したがって、複数のサーバがサービスを提供する環境において、同じクライアント識別子が2つ以上のクライアントに付与された場合でも、サーバがクライアントを確実に識別することができる。

【0129】第9の原理において、サービスシステムは、生成手段94、格納手段95、および接続手段96を備える。生成手段94は、サーバ識別子とクライアント識別子を合成して、クライアントのマシン識別子を生成し、格納手段95は、そのマシン識別子を格納する。そして、接続手段96は、そのマシン識別子を用いてサーバに接続する。

【0130】生成手段94がサーバ識別子を含むマシン識別子を生成し、接続手段96がそのマシン識別子を用いてサーバに接続することで、サーバは、その接続要求がどのサーバに対するものかを特定することができる。したがって、第8の原理と同様に、サーバがクライアントを確実に識別することができる。

【0131】第10の原理において、サービスシステムは、通信手段97と認証手段98を備える。通信手段97は、サーバへのログイン時に、そのサーバの認証鍵に基づく電子署名機能を用いて暗号化された指定情報を送受信し、認証手段98は、その指定情報を介してサーバの認証を行う。

【0132】サーバは、例えばリモートインストールサービスを提供し、ログイン一画面において、クライアントから指定された情報を秘密鍵で暗号化して送り返す。認証手段98は、その指定情報を対応する公開鍵で復号化し、その結果に基づいてサーバが正しいかどうかを判断する。復号化された情報が元の指定情報と一致すれば、サーバは正しいと判定される。

【0133】正しいサーバのみが正しい暗号化を行なうこ

とができるので、インターネットにおいて、クライアントがサーバを確実に識別することが可能になる。また、クライアントが公開鍵で暗号化した指定情報をサーバに送り、サーバがそれを秘密鍵で復号化して送り返しても、同様の効果が得られる。

【0134】第11の原理において、サービスシステムは、格納手段99と接続手段100を備え、リモートインストールサービスを提供する。格納手段99は、クライアント側に設けられ、インターネットにおけるサーバのアドレス情報を格納し、接続手段100は、上記アドレス情報を用いて、自動的に上記クライアントから上記サーバに接続する。

【0135】リモートインストールシステムのサーバのアドレス情報を(ドメイン名やポート番号)が、ホームページではなく、ユーザ端末内の格納手段99に格納されているので、他のユーザに知られることがない。このアドレス情報を、RIS会員になったユーザの端末にのみ格納することで、インターネットにおいて、会員制のリモートインストールサービスが実現される。

【0136】このように、図1のサービスシステムによれば、インターネット上でリモートインストールシステムを利用した様々な会員制サービスを、安全かつ適切に提供することが可能になる。

【0137】図1の登録手段80、キー情報付与手段81、暗号化手段82、リモートインストール手段83、ブラウザ手段88、課金手段84、処理手段85、ヘルバ手段86、処理手段87、処理手段89、処理手段90、トランザクション手段91、受信手段92、判定手段93、生成手段94、接続手段96、格納手段95、

30 通信手段97、認証手段98、格納手段99、および接続手段100は、例えば、後述する図2におけるホスト計算機111およびユーザ端末113の持つ機能に対応する。

【0138】

【発明の実施の形態】以下、図面を参照しながら、本発明の実施の形態を詳細に説明する。図2は、実施形態のサービスシステムの構成図である。図2のサービスシステムは、インターネット117に接続されたホスト計算機111およびユーザ端末113は、インターネット117以外にも、セキュリティの確保された通信路(ハイブ)であるFENICS回線116を介して互いに接続されている。

【0139】ホスト計算機111は、リモートインストールサービスを提供するソフトウェアとして、RISサーバ112を搭載し、ユーザ端末113は、WWWブラウザ114の他に、リモートインストールサービスを利用するソフトウェアとして、RISクライアント115を搭載する。

【0140】図3は、図2のホスト計算機111および

ユーザ端末113に対応する情報処理装置（コンピュータ）の構成図である。図3の情報処理装置は、CPU（中央処理装置）121、メモリ122、入力装置123、出力装置124、外部記憶装置125、媒体駆動装置126、ネットワーク接続装置127を備え、それらの各装置はバス128により互いに結合されている。

【0141】CPU121は、メモリ122を利用してプログラムを実行し、サービスに必要な処理を実現する。メモリ122には、サービスに必要なプログラムとデータが格納され、メモリ122としては、例えばROM (read only memory)、RAM (random access memory) 等が用いられる。

【0142】入力装置122は、例えばキーボード、ボイントイングデバイス等に相当し、ユーザからの要求や指示の入力に用いられる。また、出力装置124は、表示装置やプリンタ等に相当し、サービス画面等の出力に用いられる。

【0143】外部記憶装置125は、例えば、磁気ディスク装置、光ディスク装置、光磁気ディスク装置等である。この外部記憶装置125に、上述のプログラムとデータを格納しておき、必要に応じて、メモリ122にロードして使用することもできる。また、外部記憶装置125はデータベースとしても使用される。

【0144】媒体駆動装置126は、可搬記録媒体129を駆動し、その記録内容にアクセスする。可搬記録媒体129としては、メモリカード、フロッピーディスク、CD-ROM (compact disk read only memory)、光ディスク、光磁気ディスク等、任意のコンピュータ読み取り可能な記録媒体を使用することができる。この可搬記録媒体129に、上述のプログラムとデータを格納しておき、必要に応じて、メモリ122にロードして使用することもできる。

【0145】ネットワーク接続装置127は、FENICS回線116やインターネット117への接続に用いられ、伝信に伴うデータ変換等を行って、他の情報処理装置（ホスト計算機111またはユーザ端末113）との間でプログラムやデータの送受信を行なう。また、情報処理装置は、外部の情報提供者のデータベース130等からネットワークを介して、上述のプログラムとデータを受け取り、必要に応じて、メモリ122にロードして使用することもできる。

【0146】本実施形態では、システムへの登録手続き（サインアップ）は、必ずセキュリティの確保されたパイプで行なう。そして、サインアップの過程で、RISサーバ112は、ユーザID/パスワードおよびマシンID/パスワードとともに、マシンIDに対応したインターネット用の暗号キーをRISクライアント115に付与する。この暗号キーを用いて、インターネット上のパスワードおよびコンテンツの暗号化/復号化が行われる。

【0147】このようなサービスを実現するため、図4 7、48のサインアップのシーケンスに図4に示すようなシーケンスを追加し、RISサーバ112が、端末（マシン）113にユニークに対応した秘密キー（例えばDESキー）を、端末113に付与する。

【0148】図4において、RISクライアント115

が、マシンID（MID）なしでコマンドRES_SENDENVをRISサーバ112に送ると、RISサーバ112は、秘密キーデータベース131を参照してレスポンスを返す。秘密キーデータベース131には、あらかじめMIDと秘密キーの対応表が格納されている。【0149】ここでは、レスポンスとして、MID=1234、MP_SWD=ASDF、KEY=9876がRISクライアント115に返される。このうち、KEYが秘密キーに対応する。RISクライアント115は、受け取ったこれらの情報を初期設定ファイル132（RIS.INI）に書き込んで保存する。

【0150】さらに、この初期設定ファイル132には、図5に示すように、インターネット117を介してRISサーバ112に接続するためのアドレス（ドメイン名）およびTCP/IP（transmission control protocol/internet protocol）のポート番号が記述されている。

【0151】これらのアドレスとポート番号は、ユーザがRIS会員になって、RISクライアント115が端末113にインストールされた時に、端末113の初期設定ファイル132に書き込まれる。アドレス情報が、インターネット上ではなく、RISクライアント115側に保持されているので、会員以外の他のユーザにハッキングされることはない。したがって、RIS会員のみがRISサーバ112にアクセスすることができる。

【0152】このアドレス情報を用いたインターネット117でのログインは、図6に示すようなシーケンスにて行われる。RISサーバ112からユーザID（UID）の入力指示を受け取ると、RISクライアント115は、まず、UIDとともにMIDを送出す。

【0153】RISサーバ112は、Challenge発生関数133を用いて、毎回異なる乱数Challengeを生成し、RISクライアント115に送る。

40 この乱数はRISサーバ112の識別情報として送られるが、毎回異なるため、他人がハッキングして使用することができない。したがって、他のサーバがRISサーバ112になりますことを防止できる。

【0154】RISクライアント115は、合成関数134を用いて、RISサーバ112から送られたChallengeとサインアップ時に取得したKEYとを合算し、暗号化キーを生成する。合成関数134としては、例えばEOR(exclusivcor)が用いられる。そして、この暗号化キーをDES(Data Encryption Standard)アルゴリズムの秘密キー（DESキー）として用い

て、ユーザパスワードを暗号化プログラム135により暗号化し、RISサーバ112に送出する。

【0155】RISサーバ112は、RISクライアント115に送ったChallengeおよびKEYから同様にしてDESキーを合成する。そして、復号化プログラム136により、暗号化されたユーザパスワードを復号化し、ユーザパスワードの確認を行う。ユーザパスワードが暗号化されてやり取りされるため、インターネット117上でのログインにおいて、ユーザパスワードの盗用が防止される。

【0156】また、インターネット117上のコンテンツの配送においては、図44、45、46の従来のリモートインストール方法を図7に示すように拡張する。まず、RISクライアント115が、インターネット117を介して、セキュリティを要求されるコンテンツのデストリビューションを要求すると、RISサーバ112は、代金の与信を行う。

【0157】次に、RISサーバ112は、圧縮されたコンテンツファイルABC、LZHを、MIDに対応する秘密キーを用いて暗号化プログラム135により暗号化し、RISクライアント115にダウンロードする。そして、暗号化されたコンテンツファイルABC、DESを復号化するコマンドを送る。

【0158】RISクライアント115は、コンテンツファイルABC、DESを、保持しているKEYを用いて復号化プログラム136により復号化し、ファイルABC、LZHを取り出す。次に、RISサーバ112からのコマンドに従って、ファイルABC、LZHを解凍し、実行用ファイルABC.EXEを生成する。その後、ABC、DESとABC、LZHは自動的に消去される。

【0159】このように、あらかじめセキュリティの確保された通信路を介して秘密キーを送ることで、DESアルゴリズムのように堅牢な暗号化アルゴリズムを採用することができる。また、暗号化アルゴリズムとしては、秘密キーを用いる他の任意のアルゴリズムを用いることができる。

【0160】次に、ブラウザのヘルパ・アプリケーションを起動することにより、指定されたソフトウェアを配送するリモートインストールシステムについて述べる。このシステムでは、RISクライアント115をWWWブラウザ114にヘルパ・アプリケーションとしてあらかじめ登録しておく。ここで、ヘルパ・アプリケーションとは、WWWブラウザ114からキックされて起動し、それに組み込まれた機能以外の形式のファイルを表示することのできるプログラムを意味する。

【0161】そして、ホームページ上にヘルパ起動のためのアンカーファイルを置き、そのアンカーファイルをユーザがボイントイング・デバイスでクリックすると、RISクライアント115が自動的にRISサーバ11

50

2に接続し、指定のソフトウェアが配達されるようにする。

【0162】図8は、このようなインターネット117上のソフトウェア配達システムを示している。ソフトウェアのベンダであるソフト工房141は、インターネット117上にホームページ142を開き、自社の開発したソフトウェアの宣伝を行う(処理P1)。それとともに、自社の開発したソフトウェアを、図51、52に示した先頭の方法でRISサーバ112に登録する(処理P1)。

【0163】このホームページ142を構成するHTML(hypertext markup language)ファイルは、図9のように記述される。これにより、“競馬ソフト”、“バチンコソフト”等のソフトウェア名とそれらの配達を受けるための選択ボタン(Risアイコン)が表示される。これらのRisボタンには、それぞれヘルパ起動のためのアンカーファイルがリファレンスとして設定されている。

【0164】例えば、“競馬ソフト”的Risアイコン143には、図10に示すようなアンカーファイル144(KEIBA.RIS)がリンクされている。このKEIBA.RISの[RIS]セクションには、ソフトウェア名とソフトウェア番号(Soft)とが記述される。

【0165】また、アンカーファイル144におけるWWWサーバのMIME(multipurpose internet mail extensions)設定として、ファイルタイプ“RIS”が MIMEタイプ“application/x-ris”に対応付けられる。MIMEとは、WWWにおいて様々なファイル形式を扱うための方法である。これにより、WWWブラウザ114がこのリファレンスを参照してきたとき、対応するWWWサーバが、MIMEタイプとして“application/x-ris”を返すようになる。

【0166】ユーザ側は、図47、48、4の方法にて、RIS会員として既にユーザID/パスワードおよびマシンID/パスワードが付与されているものとする。また、WWWブラウザ114に、RISクライアント115をヘルパ・アプリケーションとして登録しておく。

【0167】例えば、WWWブラウザ114としてNetscapeを用いた場合は、File-Typeとして“RIS”を登録し、MIME-TYPEとして“application/x-ris”を登録する。また、RISクライアント115を起動するLaunchアプリケーションとして、“C:\\$RISW410\\$RISWIN32\RISANC32.EXE”と登録する。

【0168】この状態で、ユーザがソフト工房ホームページ142にアクセスし(処理P2)、“競馬ソフト”

の横のR i sアイコン143を、ポイントティング・デバイスでクリックしたとする(処理P3)。このとき、WWWブラウザ114は、自動的にR i Sクライアント115を起動し、R i Sクライアント115にファイルKEIBA.R i Sの内容を渡す(処理P4)。

【0169】起動されたR i Sクライアント115は、図6に示した方法でR i Sサーバ112に接続する(処理P5)。そして、ログイン後は、図11に示すように、図4、45、46と同じシケンで、R i Sサーバ112がソフトウェアのデストリビューションを行う。このとき、ファイルKEIBA.R i Sから抽出されたソフトウェア番号が、R i Sクライアント115からR i Sサーバ112に送られ、それに応するソフトウェアが自動的に端末113に配達される。

【0170】以上の操作が行われると、R i Sサーバ112上のデータベースには、図12の購入テーブルおよび図13の支払いテーブルに記述されたような購入履歴が残る。そこで、R i Sサーバ112は、この購入テーブルを元に、クレジット会社経由で購入者から代金を徵収し、支払いテーブルを元に、ベンダに払いもどしを行う(処理P6)。

【0171】このように、R i Sクライアント115をWWWブラウザ114から起動されるヘルパ・アプリケーションとして登録しておくことで、インターネット117上でのソフトウェア配送システムが実現される。また、R i Sクライアント115をヘルパとして組み込み代わりに、それをWWWブラウザ114のプラグイン(ブラウザウインドウ内のアプリケーション)として登録しておいてよい。

【0172】次に、ブラウザのヘルパ・アプリケーションを起動することにより、物品の購入を簡便に行うことのできるオンラインショッピングシステムについて述べる。このシステムでは、R i Sクライアント115をWWWブラウザ114にヘルパとして登録するとともに、ホームページ上にヘルパ起動のためのアンカーファイルを置く。

【0173】そして、このアンカーファイルをユーザがクリックすると、自動的にR i Sクライアント115がR i Sサーバ112に接続し、R i Sサーバ112は自動的に指定の商品の課金処理を行って、ベンダに購入報告を行う。ベンダは、これを受けて商品をユーザに発送する。

【0174】図14は、このようなオンラインショッピングシステムを示している。ベンダであるα商店151は、インターネット117上にホームページ152を開き、自社の扱う“タオルセット”や“ハンカチーフ”等の商品の宣伝を行なう(処理P11)。それとともに、商品の購入処理のソフトウェアを、図51、52に示した先頭の方法でR i Sサーバ112に登録する(処理P12)。

10 20

【0175】ホームページ152のHTMLファイルは、図9と同様の形式で記述され、商品の選択／購入に必要なR i sアイコンをホームページ152上に表示させる(処理P13)。それぞれのR i sアイコンにリンクしたアンカーファイルおよびユーザ側のMIME等の設定は、上述のソフトウェア配送システムと同様である。例えば、R i sアイコン153には、アンカーファイル154(TOWEL.R i S)がリンクされている。

【0176】この状態で、ユーザがα商店ホームページ152にアクセスし(処理P14)、“タオルセット”の横のR i sアイコン153をクリックしたとする(処理P15)。このとき、WWWブラウザ114は、ヘルパーとして登録されたR i Sクライアント115を起動し、R i Sクライアント115にファイルTOWEL.R i Sの内容を渡す(処理P16)。

【0177】起動されたR i Sクライアント115は、R i Sサーバ112に接続し、暗号化されたパスワードでログインして、登録されたリモートインストール処理(R i S_INSTAL L)を開始する(処理P17)。ログイン時の設定内容や手順も、上述のソフトウェア配送システムと同様である。

【0178】開始されたリモートインストール処理では、ソフトウェアの宅配の場合とは異なる動作を行うよう、そのスクリプトを記述しておく。この場合、具体的には、ユーザへ受付票を送付する処理とベンダへ購入通知を送付する処理とが、ソフトウェア配送処理の代わりに記述される。また、必要であれば、商品の発送先をユーザが指定できるようにしておく。

【0179】受付票は、ソフトウェアをダウンロードする場合と同様の方法でユーザへ送付される(処理P18)。また、購入通知は、電子メールや専用回線を介した規定フォーマットの通知票としてベンダへ送付される(処理P18)。購入通知の送付処理は、ベンダ側から見ると商品の受注処理となる。この購入通知送付処理も、リモートインストール処理中に同時に実行される。

【0180】図15は、これらの送付処理のシケンを示している。まず、R i Sクライアント115は、ファイルTOWEL.R i Sから抽出したソフトウェア番号を、注文する商品の番号としてR i Sサーバ112に送る。このとき、コマンドR i S_CHKENVを利用する。

【0181】次に、R i Sサーバ112が、レスポンスとして商品の発送先を問い合わせてくると、ユーザは希望する住所／宛て名を入力する。入力された発送先は、コマンドR i S_CHKENVを利用してR i Sサーバ112に送られる。そして、R i Sサーバ112から“OK”が返されると、R i Sクライアント115がコマンドR i S_INSTAL Lを送る。

【0182】このとき、R i Sサーバ112は、受付票

30 40 50

をダウンロードし、購入通知をベンダに送付する。そして、購入通知を受け取ったベンダは、所定の方法でユーザに商品を発送する（処理P 19）。図15の処理が終了すると、図12、13と同様の購入テーブル、支払テーブルが作成されるので、R I Sサーバ112は、これらを元にユーザから代金を徴収し、ベンダへの支払いを行う（処理P 20）。

【0183】このようなに、R I Sクライアント115をWWWブラウザ114から起動されるヘルパ・アプリケーションとして登録しておくことで、インターネット117上でのオンラインショッピングシステムが実現される。また、R I Sクライアント115をWWWブラウザ114のプラグインとして登録しておくことも可能である。

【0184】このようなシステムによれば、R I S会員としてのユーザ情報があらかじめ登録されているので、ユーザは商品の購入に際し、気に入った商品のボタンを押すだけよい。このため、非常に簡単なオンラインショッピングが可能となる。また、登録時の連絡先と異なる発送先を指定することもでき、例えば、商品を第3者への贈答品として配達させることもできる。

【0185】また、R I Sのセンターは、販売に関わる一部の業務をアウトソーシングの形で譲り負うことが可能である。したがって、個々のカード会社との契約等の煩わしい手間が省けるというメリットがある。

【0186】次に、ブラウザのヘルパ・アプリケーションを起動することにより、特定のパスワードを通してオンライン通信サービスシステムについて述べる。このシステムでは、R I Sクライアント115をWWWブラウザ114にヘルペとして登録するとともに、ホームページ上にヘルパ起動のアンカーファイルを置く。

【0187】そして、ユーザがこのアンカーファイルをクリックすると、R I Sクライアント115が自動的にR I Sサーバ112に接続する。R I Sサーバ112は、指定された通信サービスの課金処理を行い、ベンダに購入報告を行うとともに、ユーザにサービス利用のためのパスワードを通告する。ユーザは、このパスワードをWWWブラウザ114の画面に入力することで、そのサービスが受けられるようになる。

【0188】図16は、このようなオンライン通信サービスシステムを示している。通信サービスのベンダである占いの館161は、インターネット117上にホームページ162を開き、これを自社の占いサービスの受付画面とする（処理P 21）。また、占いサービスの利用権を表す占いチケットとなるパスワード情報を、図51、52に示した方法で、ユーザへの通告としてR I Sサーバ112に登録する（処理P 21）。

【0189】ホームページ162のHTMLファイルは、図17のように記述される。これにより、占いチケ

ットに対応するR i sアイコン163と、パスワードの入力欄164が表示される。R i sアイコン163には、ヘルパ起動のためのアンカーファイル165（F T E L L, R I S）がリファレンスとして設定されている。

【0190】このファイルF T E L L, R I Sの[R I S]セクションには、図18に示すように、占いサービスのサービス名とソフトウェア番号（S o f t）とが記述される。このソフトウェア番号は、サービスの識別番号として用いられる。

【0191】また、アンカーファイル165におけるW W WサーバのM I M E設定は、上述のソフトウェア配送システムと同様にしておく。これにより、WWWブラウザ114がこのリファレンスを参照してきたとき、対応するWWWサーバはM I M Eタイプとしてa p p l i c a t i o n /x - r i sを返すようになる。

【0192】ユーザ側は、上述のソフトウェア配送システムと同様に、R I S会員として既にユーザID/パスワードおよびマシンID/パスワードが付与されているものとする。さらに、WWWブラウザ114に、R I Sクライアント115をヘルパ・アプリケーションとして登録しておく。

【0193】この状態で、ユーザが占いの館ホームページ162にアクセスし（処理P 22）、占いチケットの横のR i sアイコン163をクリックしたとする（処理P 23）。このとき、WWWブラウザ114は、R I Sクライアント115を起動し、R I Sクライアント115にファイルF T E L L, R I Sの内容を渡す（処理P 24）。

【0194】起動されたR I Sクライアント115は、R I Sサーバ112に接続し、暗号化されたパスワードでログインする。インターネット117上のログインのシーケンスやR I Sクライアント115を使用するための設定は、図4、5、6に示した方法と同様である。

【0195】ログインの後、R I Sクライアント115は、ファイルF T E L L, R I Sに記述されたソフトウェア番号をR I Sサーバ112に送り（処理P 25）、R I Sサーバ112は、その番号により指定されるサービスの購入代金の課金処理を行い、その後、サービス購入者を識別するためのパスワードをユーザへ通告する（処理P 26）。

【0196】パスワードの通告は、R I Sセンターからユーザへの連絡であり、例えば図19に示すような画面を、メッセージボックスの形式で端末113上に表示することで行われる。

【0197】ユーザは、受け取ったパスワードをホームページ162上に表示された入力欄164に入力することで、対応するWWWサーバを通じて占いサービスを受けることができるようになる（処理P 27）。このために、占いサービスを提供するWWWサーバ側では、パス

ワード欄の値を得て、サービスの利用権を確認する機能を持っている。

【0198】この機能の実現方法としては、図17のHTMLファイルに記述されているCGI(common gateway interface)のスクリプトファイルura.cgiを利用。ファイルura.cgiには、図20に示すようなサービス利用権の確認処理のロジックが記述される。

【0199】確認処理が開始されると、WWWサーバ上のCGIプロセスは、まず入力されたパスワードの値を取得し(ステップS201)、それをRISサーバ112に登録したパスワードと比較して、正しいパスワードかどうかを確認する(ステップS202)。

【0200】パスワードが正しければ、そのユーザは課金されているものとみなし、有料の占いサービス提供画面を表示して(ステップS203)、処理を終了する。パスワードが正しくなければ、その誤りを指摘するメッセージをホームページ162上に表示して(ステップS204)、処理を終了する。

【0201】このような通信サービスにおけるパスワードの運用態勢としては、すべてのユーザに共通のパスワードを与えて運用し続ける方法が考えられる。また、ユーザ間でのパスワードの漏洩またはパスワード推測による不正使用の防止するため、およびサービスの提供期間を限定するために、一定期間(数分、数時間、数日等)毎にパスワードを変更する方法やユーザ毎に異なるパスワードを発行する方法などもある。また、これらのパスワード保護方法を併せて用いることもできる。

【0202】さらに、RISサーバ112への登録時に、パスワードを固定した情報とするのではなく、特定の計算アルゴリズムを用いて、パスワードを動的に生成することも可能である。

【0203】以上の操作が行われると、RISサーバ112のデータベースには、図12、13と同様のサービス購入履歴が残る。そのサービス購入履歴を元に、上述のソフトウェア配送システムと同様の手順で、購入代金が決算される(処理P28)。

【0204】このように、RISクライアント115をWWWブラウザ114から起動されるヘルパ・アプリケーションとして登録しておくことで、インターネット17上でのオンライン通信サービスシステムが実現される。また、RISクライアント115をWWWブラウザ114のプラグインとして登録しておくことも可能である。

【0205】図16のシステムでは、ユーザにパスワードを知らせることで通信サービスの利用権を与えるが、その代わりに、サービスを受けるためのURL(uniform resource locator)を通知することも考えられる。URLとは、ネットワーク上の資源を統一的に表現する識別情報である。

【0206】この場合、RISサーバ112は、課金処理後に、通信サービスのURLをユーザに通知する。そして、このURLは、課金を受けたものだけが知り得るように運用しておく。例えばURLを頻繁に変更すれば、ユーザは最新のURLを知るためにチケットを購入しなければならなくなる。

【0207】図21は、このような通信サービスシステムを示している。このシステムの動作は、基本的に図16のシステムと同様である。まず、占いの館161は、インターネット17上にホームページ166を開き、これを自社の占いサービスの受付画面とする(処理P31)。また、占いチケットとなるURL情報を、図51、52に示した方法で、RISサーバ112に登録する(処理P31)。

【0208】ホームページ166には、占いチケットに対応するRISアイコン167と、「チケット購入で占いの部屋へのURLが表示されます」というメッセージが表示される。RISアイコン167には、ヘルパ起動のためのアンカーファイル165(図18のFTEL.RIS)がリファレンスとして設定されている。

【0209】ユーザが占いの館ホームページ166にアクセスし(処理P32)、占いチケットの横のRISアイコン167をクリックしたとする(処理P33)。このとき、WWWブラウザ114は、RISクライアント115を起動し、RISクライアント115にファイルFTEL.RISの内容を検索(処理P34)。

【0210】起動されたRISクライアント115は、RISサーバ112に接続し、暗号化されたパスワードでログインし、ファイルFTEL.RISに記述されたソフトウェア番号をRISサーバ112に送る(処理P35)。RISサーバ112は、その番号により指定されるサービスの購入代金の課金処理を行い、その後、占いサービスページ168のURLをユーザへ通告する(処理P36)。URLの通告は、例えば図19と同様のメッセージボックスを用いて行われる。

【0211】ユーザは、通告によって知り得た占いサービスへのURLをWWWブラウザ114上で指定することで、そのサービスページ168にアクセスして、占いサービスを受けることができるようになる(処理P37)。

【0212】また、図21のシステムにおいて、URLをユーザに通知する代わりに、そのURLを参照するブラウザを自動的に起動することも可能である。この場合、RISセンターからのURL通知をトリガとして、ソフトウェアよりブラウザを起動することで、ユーザがURLを直接扱うことなく、URLに対応したサービス画面へのアクセスが可能になる。

【0213】WWWブラウザ114の実装形態により、すでに起動されているWWWブラウザ114が、外部からのイベントによりURL指定を自動取得可能な場合

は、R I S クライアント 1 1 5 は、WWW ブラウザ 1 1 4 が読み込み可能な形式で U R L をそれに通知する。このような方法としては、例えば、WWW ブラウザ 1 1 4 の所定のファイルに U R L を書き込んだ後、動作している WWW ブラウザ 1 1 4 にソフトウェアシグナルを送付する方法がある。

【0 2 1 4】 W I N 9 5 (W i n d o w s 9 5) の場合は、例えば図 2 2 に示すようなファイル W O R K . U R L を作成する。このファイル W O R K . U R L には、モザイク、N E T S C A P E 等のブラウザのタイプに応じて、R I S サーバ 1 1 2 から通知された U R L が書き込まれる。

【0 2 1 5】 そして、R I S クライアント 1 1 5 は、W I N 9 5 の A P I (application programming interface) を使用して、WWW ブラウザ 1 1 4 を立ち上げる。A P I とは、オペレーティングシステムが提供するプロダミング・インターフェースである。

【0 2 1 6】 この場合の A P I は、例えば “ S h e l l Execute (~, ” W O R K , U R L ”, ~) ” のように記述される。これにより、WWW ブラウザ 1 1 4 は、ファイル W O R K . U R L から自動的に U R L を取得して、対応するサービス画面にアクセスする。

【0 2 1 7】 また、WWW ブラウザ 1 1 4 が、上述の方法で、ソフトウェア的に U R L 指定を自動取得可能でない場合は、所定の U R L を初期 U R L 引数として与えて、R I S クライアント 1 1 5 から別途 WWW ブラウザ 1 1 4 を起動する。複数の WWW ブラウザ 1 1 4 が同時に並行して動作すると不都合がある場合は、以前から動作していた WWW ブラウザ 1 1 4 を一旦終了させ、その後で改めて WWW ブラウザ 1 1 4 を起動すればよい。

【0 2 1 8】 次に、トランザクション用ヘルパと R I S システムとで構成するトランザクション処理システムについて述べる。このシステムでは、トランザクション用ヘルパを用意し、トランザクション用の使用権を R I S システムに登録しておく。そして、ヘルパとして起動された R I S システムが、トランザクション用の別ヘルパと連携することにより、トランザクション処理の使用権のデストリビューションと譲り受け処理を行う。

【0 2 1 9】 図 2 3 は、このようなトランザクション処理システムを示している。ベンダーである V O I C E 工房の WWW サーバ 1 1 1 は、例えば入力されたユーザの音声を元に占いを実行する音声占いのトランザクションサービスを提供する。まず、WWW サーバ 1 1 1 は、音声占いのホームページ 1 7 2 をインターネット 1 1 7 上に開き、そのトランザクションサービスの使用権を表す音声占い券を、ソフトウェアとして R I S サーバ 1 1 2 に登録する（処理 P 4 1 ）。

【0 2 2 0】 また、ユーザ端末 1 1 3 上では、WWW ブラウザ 1 1 4 のヘルパとして、R I S クライアント 1 1 5 と V o i c e 処理プログラム 1 7 8 が登録される。V

o i c e 処理プログラム 1 7 8 は、ユーザから音声の入力を受けて、各種フィルタリング処理の後、音声ファイルを作成する専用のソフトウェアであり、V O I C E 工房により作成/配布される。

【0 2 2 1】 ユーザは、まず、WWW ブラウザ 1 1 4 から V O I C E 工房ホームページ 1 7 2 にアクセスし（処理 P 4 2 ）、音声占い券販売のアイコン 1 7 3 をクリックする（処理 P 4 3 ）。

【0 2 2 2】 このアイコン 1 7 3 には、R I S クライアント 1 1 5 を起動するためのアンカーファイル 1 7 6 (U R A N A . R I S) がリファレンスとして設定されており、WWW ブラウザ 1 1 4 は、R I S クライアント 1 1 5 を起動して、ファイル U R A N A . R I S の内容を渡す（処理 P 4 4 ）。ファイル U R A N A . R I S における M I M E 設定は、図 8 のシステムと同様である。

【0 2 2 3】 起動された R I S クライアント 1 1 5 は、インターネット 1 1 7 を介して R I S サーバ 1 1 2 に接続し（処理 P 4 5 ）、ダイレクトに音声占い券のデストリビューションを行う。

【0 2 2 4】 ここでは、デストリビューション処理として、R I S クライアント 1 1 5 が V o i c e 処理プログラム 1 7 8 の初期設定ファイル 1 7 9 (V o i c e . i n i) の情報を書き換える（処理 P 4 6 ）。例えば、ファイル V o i c e . i n i の [P e r m i s s i o n] セクションに “ Y E S ” を書き込むことで、音声占い券のデストリビューションが行われ、ユーザにサービスの利用権が与えられる。

【0 2 2 5】 次に、ユーザがホームページ 1 7 2 の音声入力開始のアイコン 1 7 4 をクリックする（処理 P 4 7 ）。このアイコン 1 7 4 には、V o i c e 処理プログラム 1 7 8 を起動するためのアンカーファイル 1 7 7 (K U B O . V O C) がリファレンスとして設定されており、WWW ブラウザ 1 1 4 は、V o i c e 処理プログラム 1 7 8 を起動する（処理 P 4 8 ）。アンカーファイル 1 7 7 における M I M E 設定として、ファイルタイプ “ . V O C ” が M I M E タイプ “ a p p l i c a t i o n / x - v o i c e ” に対応付けられている。

【0 2 2 6】 起動された V o i c e 処理プログラム 1 7 8 は、図 2 4 に示すような処理を行う。V o i c e 処理プログラム 1 7 8 は、まず、初期設定ファイル 1 7 9 の [P e r m i s s i o n] セクションに “ Y E S ” と記述されているかどうかを調べる（ステップ S 2 1 1 ）。ここに “ Y E S ” と記述されていなければ、“占い券未購入” というメッセージを表示して（ステップ S 2 1 6 ）、処理を終了する。

【0 2 2 7】 ここで “ Y E S ” と記述されていれば、音声入力動作を開始し（ステップ S 2 1 2 ）、入力音声のフィルタリング等の各種ローカル処理を行って（ステップ S 2 1 3 ）、音声ファイル（不図示）を生成/出力する（ステップ S 2 1 4 ）。そして、ファイル V o i c e

e. ini の [Permission] セクションの “YES” を消去し (ステップ S 215) 、処理を終了する。

【0228】こうして、音声ファイルが送出されると、ユーザは、次に占い開始のアイコン 175 をクリックし、占いサービスを実行する (処理 P 49)。占い開始のページは、例えば図 25 に示すように構成される。図 25においては、音声ファイル名入力欄 181、Browse アイコン 182、ADD アイコン 183、および実行アイコン 184 が表示されている。

【0229】Browse アイコン 182 がクリックされると、ファイルセレクタ 185 が開き、ここで選択された音声ファイル名が自動的に入力欄 181 に人力される。ADD アイコン 183 は、入力する音声ファイルを追加する際に用いられる。HTML ファイル 186 は、この占い開始ページの記述方法を表す。

【0230】ユーザにより音声ファイル名が入力され、実行アイコン 184 がクリックされると、指定された音声ファイルが占いサービスを行なう WWW サーバ 171 にアップロードされる。音声ファイルのアップロードは、既知の HTML ファイルアップロード機能を用いて行われる。WWW サーバ 171 は、アップロードされた音声ファイルを処理して、占い結果 180 を WWW ブラウザ 114 に返す (処理 P 50)。

【0231】音声占いの使用料金は、RIS クライアント 115 が RIS サーバ 112 に接続した時点で課金処理され、その後、RIS サーバ 112 から VOICE 工房に払い戻される (処理 P 51)。

【0232】ところで、上述の初期設定ファイル 179 を利用して、ローカルなトランザクション処理プログラムから直接 RIS クライアント 115 を起動し、図 23 と同様の方法でトランザクション処理の使用権のデストリビューションと課金処理を行なうことができる。

【0233】この場合、トランザクション処理プログラムを、図 26 のフローチャートに示すように構成する。トランザクション処理プログラムは、まず、ファイル voice. ini の [Permission] セクションに、サービス使用権の購入処理中であることを示す情報 “BUYING” が書き込まれているかどうかを調べる (ステップ S 221)。

【0234】ここに “BUYING” が書かれていれば、それが消去されるまで同じ判定を繰り返し、“BUYING” が書かれていないければ、次に、その [Permission] セクションに、購入済を表す情報 “YES” が書き込まれているかどうかを調べる (ステップ S 222)。

【0235】ここに “YES” が書かれていないれば、サービス使用権 (占い券) を購入中でも購入済でもないことがわかる。そこで、トランザクション処理プログラムは、占い券を購入するかどうかをユーザに問い合わせる

(ステップ S 228)。ここで、ユーザが占い券の購入を選択しなければそのまま処理を終了する。

【0236】ユーザが占い券の購入を選択すると、トランザクション処理プログラムは、ファイル voice. ini の [Permission] セクションに “BUYING” を書き込んで (ステップ S 229)、RIS クライアント 115 を起動し (ステップ S 230)、ステップ S 228 以降の処理を繰り返す。

【0237】起動された RIS クライアント 115 は、図 23 のシステムと同様の方法で RIS サーバ 112 に接続して、占い券を購入する。占い券の購入が終わると、RIS クライアント 115 は、ファイル voice. ini の [Permission] セクションの “BUYING” を消去して、代わりに “YES” を書き込む。

【0238】このとき、ステップ S 221 の判定結果が NO となり、ステップ S 222 の判定結果が YES となる。そこで、トランザクション処理プログラムは、音声入力動作を開始し (ステップ S 223)、入力音声のフィルタリング等の処理を行なって (ステップ S 224)、占いを実行する (ステップ S 225)。

【0239】そして、占い結果を表示し (ステップ S 26)、ファイル voice. ini の [Permission] セクションの “YES” を消去して (ステップ S 227)、処理を終了する。[Permission] セクションの “YES” を消去することで、トランザクション処理は初期状態を回復する。

【0240】このように、RIS システムと連携するトランザクション処理プログラムをユーザ端末 113 上に備えることで、WWW ブラウザ 114 の介在なしに RIS システムを利用することが可能になる。

【0241】また、図 23 のトランザクションサービスシステムにおいて、複数回のサービス利用権を販売することもできる。この場合は、RIS サーバ 112 には複数回の使用権を登録しておき、Voice 处理プログラム 178 前では、トランザクション処理毎に、初期設定ファイルのカウント数を 1 だけデクリメントする構成を用いる。

【0242】図 27 は、このようなトランザクションサービスシステムを示している。図 27 のシステムにおいては、RIS サーバ 112 には、1 回、5 回、10 回の 3 種類の占い券が、それぞれ、ソフトウェア番号 160、161、162 に対応して登録されている。そして、ベンダの VOICE 工房ホームページ 191 には、音声占い券販売のアイコンとして、1 回券、5 回券、10 回券のアイコン 192、193、194 が表示される。

【0243】これらのアイコン 192、193、194 には、それぞれ、アンカーファイル 195 (URAN A. RIS)、196 (URANA2. RIS)、19

7 (URANA3, RIS) がリファレンスとして設定されている。そして、ファイルURANA, RISにはソフトウェア番号160が記述され、ファイルURANA2, RISにはソフトウェア番号161が記述され、ファイルURANA3, RISにはソフトウェア番号162が記述されている。

【0244】ユーザがいざれかの占い券を選択して、対応するアイコンをクリックすると、RISクライアント115は、そのアイコンにリンクしているアンカーファイルのソフトウェア番号をRISサーバ112に送り、初期設定ファイル179の【Permission】セクションに、対応するカウント数(Count)を書き込む。例えば、10回券が購入された場合は、Count=10となる。これにより、複数回のサービス利用権がユーザ端末113に設定される。

【0245】図28は、このシステムにおけるVoice処理プログラム178の処理のフローチャートである。Voice処理プログラム178は、まず、初期設定ファイル179の【Permission】セクションのCountの値が0かどうかを調べる(ステップS231)。Countが0であれば、「占い券未購入」というメッセージを表示して(ステップS236)、処理を終了する。

【0246】Countが0より大きければ、音声入力動作を開始し(ステップS232)、入力音声のフィルタリング等の各種ローカル処理を行って(ステップS233)、音声ファイルを生成/出力する(ステップS234)。そして、ファイルVoice.iniの【Permission】セクションのCountの値を、1だけデクリメントして(ステップS235)、処理を終了する。

【0247】このようなVoice処理プログラム178を用いれば、ユーザは、購入したサービス利用権の利用回数だけ、サービスを受けることができる。図27のシステムにおけるその他の設定および動作は、図23のシステムと同様である。

【0248】次に、ローカルなトランザクション処理プログラムとRISシステムの連携処理により、データの取得および譲金を行うシステムについて述べる。このシステムでは、トランザクション処理プログラムから直接RISクライアント115を起動し、図23と同様の方法でトランザクション処理用のデータを入手する。

【0249】例えば、トランザクション処理プログラムが競馬予想ソフトウェアである場合、その処理のフローチャートは、図29に示すようである。競馬予想ソフトウェアは、起動時に、まず新しいデータを取得するかどうかをユーザに問い合わせる(ステップS241)。

【0250】そして、ユーザが新しいデータを取得しない意思決定を行った場合は、既存の競馬データを用いて予想を実行し(ステップS243)、処理を終了する。

また、ユーザが新しいデータを取得する意思決定を行った場合は、RISクライアント115を起動する(ステップS242)。

【0251】RISクライアント115は、ソフトウェア番号を元にしてRISサーバ112にアクセスする。RISサーバ112には、図30に示すように、競馬データがあらかじめ登録されており、図8と同様な方法で、ダイレクトに競馬データのデストリビューションを行う。そして、競馬予想ソフトウェアは、配送された競馬データを用いて予想を実行し(ステップS243)、処理を終了する。

【0252】図31は、RISクライアント115とRISサーバ112による競馬データのデストリビューション処理を示している。この処理は、図44、45、46に示した方法を利用して実行される。まず、RISクライアント115が、競馬予想ソフトウェアに付随する競馬データファイルKEIBA.DATの日付を調べ、RISサーバ112に送る(ステップS251)。ファイルKEIBA.DATには、例えば図32に示すように、競走馬等のデータA、B、Cが格納されている。

【0253】RISサーバ112は、図33に示すような日付・ファイル名対応表を参照して、送られた日付に対応するファイル名を検索し、それに対応するファイルを、追加データファイルとしてRISクライアント115に送付する(ステップS252)。そして、その内容をファイルKEIBA.DATに追加して、ファイルKEIBA.DATを更新し(ステップS253)、処理を終了する。

【0254】図33の日付・ファイル名対応表は、あらかじめRISサーバ112に登録されており、必要に応じて更新される。日付・ファイル名対応表に記載されたファイルFILE1..LZII..FILE2..LZH..FILE3..LZHには、図24に示すようなデータの組み合わせが含まれる。

【0255】例えば、ファイルFILE1..LZHにはデータD、E、F、Gが含まれ、ファイルFILE2..LZHにはデータE、F、Gが含まれ、ファイルFILE3..LZHにはデータF、Gが含まれている。このように、ファイル毎にデータの組み合わせを変えておくことで、日付の古いファイルKEIBA.DATほど、多くの追加データが与えられるようになることができる。

【0256】図29のようなトランザクション処理

プログラムによれば、WWWブラウザ114の介在なしに、RISシステムを利用してサービスに必要なデータを配

送することができる。

【0257】また、トランザクション処理プログラムが、起動時にデータファイルの日付を見て、前回のデータ更新時から一定時間経過している場合のみ、RISサーバ112に接続し、データ取得を行う構成にすることもできる。この場合、トランザクション処理プログラム

は、現在の日付がデータファイルの日付より所定日数以上経過していれば、R I Sサーバ112に接続して、最新のデータによりデータファイルを更新する。

【0258】図35は、このような競馬予想ソフトウェアのフローチャートである。競馬予想ソフトウェアは、起動時に、現在の日付とデータファイルK E I B A . D A T の日付の差を計算し、それが2ヶ月を越えているかどうかを判定する(ステップS261)。

【0259】その差が2ヶ月を越えていなければ、既存の競馬データを用いて予想を実行し(ステップS263)、処理を終了する。また、その差が2ヶ月を越えていれば、R I Sクライアント115を起動し、新しい競馬データをR I Sサーバ112から取得する(ステップS262)。そして、配送された競馬データにより更新されたファイルK E I B A . D A T を用いて、予想を実行し(ステップS263)、処理を終了する。

【0260】次に、複数のR I Sサーバ¹⁴が存在するネットワーク環境において、ユーザ端末(クライアントマシン)のマシンID(M I D)にサーバ識別子を混ぜることで、サーバによるユーザ端末の誤認識を防ぐR I Sシステムについて述べる。

【0261】このシステムでは、サーバ識別子とクライアントマシンの識別子を合成して、そのクライアントマシンを識別するM I Dを生成する。そして、サーバはクライアントから送られたM I Dをサーバ部とクライアント部に分解し、サーバ部がそのサーバの識別子と異なっていたら、クライアントとの接続を切断する。

【0262】従来のR I Sシステムによるクライアント識別の方法は、サーバがただ1つしか存在しないことを前提としていた。これに対して、本実施形態の方法を用いれば、複数のサーバがサービスを行い、1つのクライアントが各サーバに接続する場合でも、サーバによるクライアントの誤認識を防ぐことができる。

【0263】このシステムでは、それぞれ異なる複数のサーバ¹⁴は、それ自身を表す固有の識別子を有し、クライアントのM I Dは、常にアクセス先のサーバ識別子を用いて作成することにする。したがって、同じマシンでも、そのアクセス先によってM I Dが異なってくる。

【0264】図36は、サーバA、Bとクライアントマシン α 、 β を含むシステムを示している。このシステムにおいて、サーバAは、クライアント番号1に対してマシン α の情報(ディレクトリ情報やメモリ等)を保持し、クライアント番号2に対してマシン β の情報を保持する。また、他のサーバBは、クライアント番号2に対してマシン β の情報を保持し、クライアント番号1に対してマシン β の情報を保持している。

【0265】図41に示した従来の方法では、クライアント番号自体がM I Dとして使われていた。この方法をそのまま図36のシステムに適用すると、マシン α がクライアント番号1をM I DとしてサーバBに接続した場

合、サーバはそれをマシン β のM I Dとみなして、マシン α から送られる情報をマシン β の情報に上書きしてしまう事故が発生し得た。

【0266】しかし、クライアント識別子 α を混ぜてM I Dを生成することで、クライアントが誤った識別子を用いてサーバに接続した場合に、サーバ側でこれをチェックして、誤りを検出することが可能になる。これにより、サーバは、マシン情報を誤って上書きしてしまうことを避けるとともに、クライアントに対して、誤りを通知することができる。

【0267】例えば、マシン α がサーバA、Bにアクセスする際のM I Dを、それぞれ“A1”、“B2”とし、マシン β がサーバA、Bにアクセスする際のM I Dを、それぞれ“A2”、“B1”とする。

【0268】このとき、マシン α が、誤って“B2”をM I DとしてサーバAにアクセスした場合、サーバAは、まず、そのM I Dをサーバ部“B”とクライアント部“2”とに分解して、サーバ部の識別子を調べる。この場合、サーバ部“B”が自身の識別子と異なるので、このアクセスは誤りと判断し、マシン α との接続を切断する。

【0269】また、マシン α が、誤って“A1”をM I DとしてサーバBにアクセスした場合も、同様にして誤りが検出され、マシン α との接続が切断される。ここでは、アクセスの誤りを接続の切断という方法でクライアントに通知しているが、代わりにエラーメッセージ等を用いてもよい。

【0270】このシステムのサーバ識別子としては、ドメイン名r i s . g m s n e t . o r . j p のように、世界で唯一であることが保証されているものを用いることが望ましい。そうすれば、サーバ識別子の重複という事故を避けることができる。クライアントの識別を完璧に行うことができる。したがって、1つのクライアントで複数のサーバを使い分ける場合でも、クライアントのマシン情報が混乱することが避けられる。

【0271】また、このような複数のサーバの取扱いにおいて、各サーバに対応する初期設定ファイルをクライアント側に持つことも考えられる。この場合、基本となるサーバの初期設定ファイルに、他のサーバの初期設定ファイルがあるかどうかを、拡張情報として記述しておく。

【0272】例えば、図37に示すファイルR I S . 1 N I を基本の初期設定ファイルとし、図38に示すファイルR I S 2 . I N I を別のサーバの初期設定ファイルとする。このように、サーバ毎に異なる初期設定ファイルを用意すれば、矢印で示されるように、それぞれまったく異なるユーザID/パスワードおよびM I Dを扱うことができる。

【0273】また、図37のファイルR I S . I N I の中に[X T E N S I O N]セクションが設けられ、

ここに他の初期設定ファイルをアクティブにするかどうかを記述できる。ここでは、ファイルR1S.INIとR1S2.INIがアクティブ(ON)になっており、動作時には、他のファイルR1S2.INIも自動的に参照される。

【0274】図36に示した方法を用いれば、サーバ側は正しくクライアントマシンの情報をハンドリングすることができる。次に問題となるのは、クライアント側にとって、正しいサーバに接続できたかどうかを確認することにある。というのは、複数のサーバが存在する場合、間違って悪意のあるサーバに接続するかもしれないという危険性があるからである。

【0275】そこで、次に、正しいサーバを識別するR1Sシステムについて述べる。このシステムでは、RSA(Rivest-Shamir-Adleman)暗号による電子署名の機能を用いたログインセッションを設ける。RSA暗号は、非対称暗号システムであり、暗号化と復号化にはそれぞれ異なる鍵情報を用いられる。

【0276】このログインセッションにおいて、サーバは、決められた情報を秘密鍵で暗号化してクライアントに送り、クライアントは、それを公開鍵で復号化することにより、サーバの認証を行う。これにより、クライアントは、ログイン先が正しいサーバかどうかを判定することができる。

【0277】図39は、このようなサーバ識別システムを示している。図39において、各サーバは、RSAの秘密鍵を保持し、対応する公開鍵をホームページ201に登録しておく。サーバのリストを表示するホームページ201が信用できるかどうかは、ユーザが判断するものとする。あるいは、信用できるホームページ201のURLをあらかじめクライアントに埋め込んでおいてよい。

【0278】サーバは、クライアントから接続時に任意の情報を平文で渡しても、それを秘密鍵で暗号化して返すと、クライアントは、サーバの公開鍵で元の平文を正しく復元することができる。正しく復元できたということは、サーバがその公開鍵と対を成す秘密鍵を保持していることになるので、正しいサーバであると判断できる。

【0279】図39において、マシンaは、サーバAへの接続に先立ち、その識別子“A”、公開鍵“公A”等のサーバ情報を持てておらず、マシンaは、R1Sクライアント115を起動する。このとき、必要であれば、他のサーバの情報を取得しておく。

【0280】この状態で、マシンaがサーバAを識別するログインシーケンスは、図40に示すようになる。マシンaがサーバAに接続すると、サーバAはサーバ識別のための情報[Word]を問い合わせてくる。そこで、マシンaが情報“apple”を平文で送ると、サーバAはそれを秘密鍵“秘A”で暗号化し、暗(a p p l e , 秘A)

e. 秘A)として送り返す。

【0281】マシンaは、暗(a p p l e , 秘A)を公開鍵“公A”で復号化し、情報“apple”を取り出す。この情報は、先に送った情報と一致するので、接続先は正しいサーバAであると判断する。そこで、ユーザがUIDを入力し、マシンaは通常のログインシーケンスに移行する。

【0282】これに対して、サーバAになりすましたサーバ'A'に対するログインシーケンスは、図41に示すようになる。マシンaがサーバ'A'に接続して、サーバ'A'に情報“apple”を送るところまでは、図40と同様である。サーバAは、受け取った情報を、適当に設定した秘密鍵“秘A'”で暗号化し、暗(a p p l e , 秘A')として送り返す。

【0283】ところが、マシンaが暗(a p p l e , 秘A')を公開鍵“公A”で復号化すると、平文“b q q m f”が取り出される。この情報は、先に送った情報と異なるので、接続先は正しいサーバAではないと判断し、接続を切断する。こうして、偽のサーバ'A'を識別することができる。

【0284】また、図40、41のシーケンスとは異なり、クライアントがサーバの公開鍵で暗号化した情報をサーバに送り、サーバがそれを秘密鍵で復号化して、クライアントに平文として送り返しても、同様の効果が得られる。この場合、クライアントは、サーバから送り返された平文が正しければ、そのサーバを正しいサーバと認識する。

【0285】図39のサーバ識別システムにおいて、サーバ認証鍵となる公開鍵および秘密鍵を固定したまま運用を続けると、いつか暗号を破られる可能性がある。そこで、これらのを定期的に更新することにより、暗号の安全性を高める必要がある。しかし、公開鍵が変更される度に、クライアント側のサーバ情報を設定し直すのは不便なので、この過程を自動化し、クライアントがサーバにログインするときに、毎回サーバ情報を取得するようとする。

【0286】そして、図8に示した方法を利用して、ホームページからR1Sクライアント115を起動する。この場合、R1Sアイコンにリンクしたアンカーファイルは、図42に示すように拡張され、その[SERVER]セクションにサーバ識別子が記述され、[OKEY]セクションに公開鍵が記述される。

【0287】WWWブラウザ114から起動されたR1Sクライアント115は、R1Sサーバに接続する前に、図43に示すような処理を行う。R1Sクライアント115は、まず、図42のアンカーファイルR1S2.R1Sの[SERVER]セクションを見て、R1Sサーバ“0002”へのアクセス権があるかどうかを調べる(ステップS271)。

【0288】ここに、サーバ識別子“0002”が記述

されていればアクセス権があると判断し、次に、【OK E Y】セクションを見て、新たな公開鍵“1 2 3 4”を取り込む（ステップS 2 7 2）。そして、【R I S】セクションを見て、ソフトウェア番号ではなく、“S i a r t =m e n u”と記述されていることを知る。そこで、ソフトウェアを要求するではなく、初期メニューからR I Sサーバ“0 0 0 2”にアクセスすることを認識し（ステップS 2 7 3）、処理を終了する。

【0 2 8 9】ステップS 2 7 1において、サーバ“0 0 0 2”へのアクセス権がないことがわかると、エラー表示等の処理を行って（ステップS 2 7 4）、処理を終了する。こうして、ファイルR I S 2、R I Sの読み取りが終了すると、R I Sクライアント1 1 5は、図40に示したようなログインセッションを開始する。

【0 2 9 0】以上説明した実施形態において、暗号アルゴリズムはD E SとR S Aに限られず、他の任意のものを使いいることができる。また、図14のオンラインショッピングシステムでは、タオルセット、ハンカチーフ以外の任意の商品、サービスを販売することができ、図16、2 1の通信サービスシステムでは、占いサービス以外の任意の通信サービスを提供することができる。また、図2 3、2 7のトランザクションサービスシステムでは、音声占いサービス以外の任意のトランザクションサービスを提供することができる。

【0 2 9 1】

【発明の効果】本発明によれば、インターネット上でリモートインストールシステムを利用して、ソフトウェア配達サービス、オンラインショッピング、通信サービス、トランザクションサービス等の様々な会員制サービスを提供することが可能になる。また、インターネット上で接続先の認証や、パスワード、コンテンツ等の暗号化も行われ、サービスの安全性が保証される。

【図面の簡単な説明】

【図1】本発明のサービスシステムの原理図である。

【図2】実施形態のシステム構成図である。

【図3】情報処理装置の構成図である。

【図4】サインアップシーケンスを示す図である。

【図5】第1の初期設定ファイルを示す図である。

【図6】第1のログインシーケンスを示す図である。

【図7】暗号化されたコンテンツの配達を示す図である。

【図8】インターネット上のソフトウェア配達システムを示す図である。

【図9】ソフト工房ホームページのH T M Lファイルを示す図である。

【図10】第1のアンカーファイルを示す図である。

【図11】ソフトウェアの配達を示す図である。

【図12】購入テーブルを示す図である。

【図13】支払いテーブルを示す図である。

【図14】オンラインショッピングシステムを示す図で

ある。

【図15】受付票／購入通知送付処理を示す図である。

【図16】オンライン通信サービスシステムを示す図である。

【図17】占いの館ホームページのH T M Lファイルを示す図である。

【図18】第2のアンカーファイルを示す図である。

【図19】パスワードの表示画面を示す図である。

【図20】サービス利用権の確認処理のフローチャートである。

【図21】U R Lを通知する通信サービスシステムを示す図である。

【図22】U R L格納ファイルを示す図である。

【図23】第1のトランザクションサービスシステムを示す図である。

【図24】第1のV o i c e処理プログラムのフローチャートである。

【図25】占い開始画面を示す図である。

【図26】トランザクション処理プログラムのフローチャートである。

【図27】第2のトランザクションサービスシステムを示す図である。

【図28】第2のV o i c e処理プログラムのフローチャートである。

【図29】第1の競馬予想処理のフローチャートである。

【図30】R I Sサーバの情報を示す図である。

【図31】データのデストリビューション処理のフローチャートである。

【図32】競馬データファイルを示す図である。

【図33】日付・ファイル名対応表を示す図である。

【図34】各ファイルに含まれるデータを示す図である。

【図35】第2の競馬予想処理のフローチャートである。

【図36】複数のサーバが存在するシステムを示す図である。

【図37】第2の初期設定ファイルを示す図である。

【図38】第3の初期設定ファイルを示す図である。

【図39】サーバ識別システムを示す図である。

【図40】第2のログインシーケンスを示す図である。

【図41】第3のログインシーケンスを示す図である。

【図42】第3のアンカーファイルを示す図である。

【図43】クライアントの処理のフローチャートである。

【図44】リモートインストールのフローチャート（その1）である。

【図45】リモートインストールのフローチャート（その2）である。

【図46】リモートインストールのフローチャート（そ

の3)である。		8 4 課金手段
【図4 7】ユーザID登録のフローチャートである。		8 5、8 7、8 9、9 0 処理手段
【図4 8】端末ID登録のフローチャートである。		8 6 ヘルパ手段
【図4 9】販売のフローチャートである。		8 8 ブラウザ手段
【図5 0】端末パスワードチェックのフローチャートである。		9 1 トランザクション手段
【図5 1】場の構成を示す図である。		9 2 受信手段
【図5 2】作者の作業のフローチャートである。		9 3 判定手段
【図5 3】オリジナルクラブ管理者の作業のフローチャートである。		9 4 生成手段 9 4
【図5 4】転載先クラブ管理者の作業のフローチャートである。		9 5、9 9 構築手段
【図5 5】アップロードを示す図である。	10	9 6、1 0 0 接続手段
【図5 6】シェアウェア手続きを示す図(その1)である。		9 7 通信手段
【図5 7】シェアウェア手続きを示す図(その2)である。		9 8 認証手段
【図5 8】シェアウェア手続きを示す図(その3)である。		1 1 1 ホスト計算機
【図5 9】シェアウェア手続きを示す図(その4)である。	20	1 1 2 R I S サーバ
【図6 0】代金引き落とし手続きを示す図(その1)である。		1 1 3 ユーザ端末
【図6 1】代金引き落とし手続きを示す図(その2)である。		1 1 4 WWW ブラウザ
【図6 2】代金引き落とし手続きを示す図(その3)である。		1 1 5 R I S クライアント
【符号の説明】		1 1 6 F E N I C S 回線
1、2 環境ファイル		1 1 7 インターネット
3、4 キーテーブル	20	1 2 1 C P U
5 チェックスクリプト		1 2 2 メモリ
6 ファイル本体		1 2 3 入力装置
7 インストールスクリプト		1 2 4 出力装置
1 1、1 2、1 3、1 4 クラブ		1 2 5 外部記憶装置
1 5 ソフトウェア		1 2 6 媒体駆動装置
2 1 C F G ファイル		1 2 7 ネットワーク接続装置
2 2 説明ファイル		1 2 8 バス
2 3 インストール関連ファイル		1 2 9 可搬記録媒体
2 4 本体ファイル		1 3 0 データベース
2 5 定義ファイル	30	1 3 1 秘密キーデータベース
2 6 C H K ファイル		1 3 2、1 7 9 初期設定ファイル
2 7 書換えファイル		1 3 3 C h a l l e n g e 発生回数
2 8 コンテンツデータベース		1 3 4 合成閾数
2 9 メニュー		1 3 5暗号化プログラム
3 0 ダイアログボックス		1 3 6 復号化プログラム
3 1 メッセージ		1 4 1 ソフト工房
8 0 登録手段		1 4 2 ソフト工房ホームページ
8 1 キー情報付与手段		1 4 3、1 5 3、1 6 3、1 6 7、1 9 2、1 9 3、1
8 2 暗号化手段		9 4 R i s アイコン
8 3 リモートインストール手段	40	1 4 4、1 5 4、1 6 5、1 7 6、1 7 7、1 9 5、1
		9 6、1 9 7 アンカーファイル
		1 5 1 α商店
		1 5 2 α商店ホームページ
		1 6 1 占いの館
		1 6 2、1 6 6 占いの館ホームページ
		1 6 4 パスワード入力欄
		1 6 8 占いサービスページ
		1 7 1 V O I C E 工房サーバ
		1 7 2、1 9 1 V O I C E 工房ホームページ
	50	1 7 3、1 7 4、1 7 5、1 8 2、1 8 3、1 8 4 ア

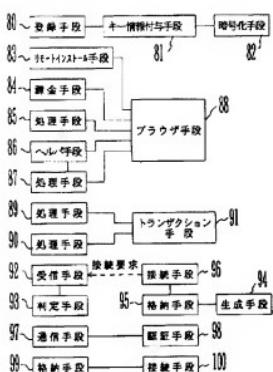
イコン
178 Voice処理プログラム
180 古い結果
181 音声ファイル名入力欄

* 185 ファイルセレクタ
186 HTMLファイル
201 信用できるホームページ

*

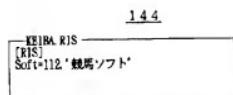
【図1】

本発明の原理図



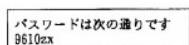
【図10】

第1のアンカーファイルを示す図



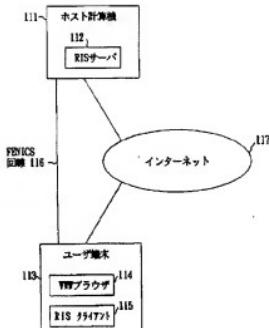
【図19】

パスワードの表示画面を示す図



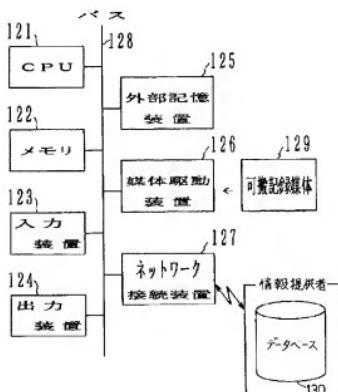
【図2】

システム構成図



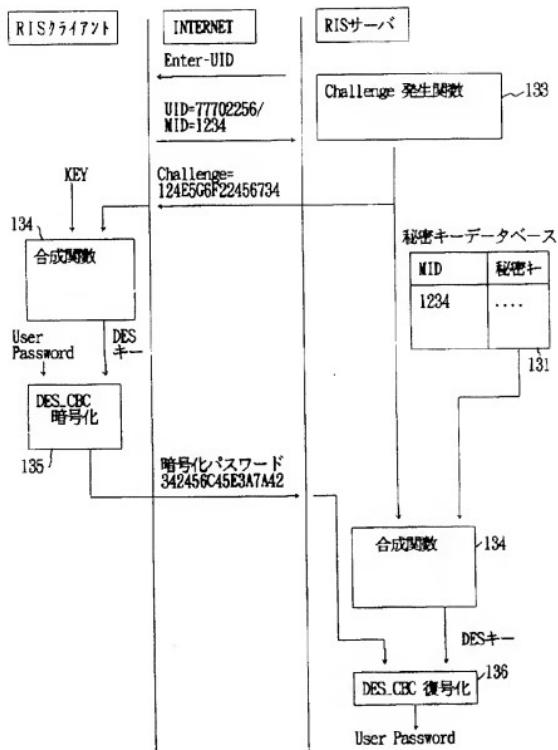
【図3】

情報処理装置の構成図



【図6】

第1のログインシーケンスを示す図



【図13】

支払いテーブルを示す図

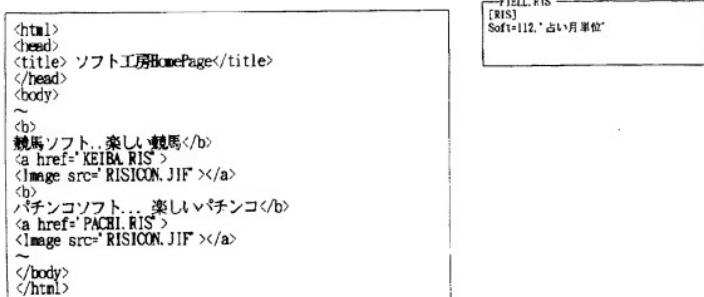
消費者ID	ベンダID	品目	原価	数量	日付
77702256	125457	競馬ソフト	4000	1	96.10.25

[图9]

[図-8]

ソフト工房ホームページのHTMLファイルを示す図 第2のアンカーファイルを示す図

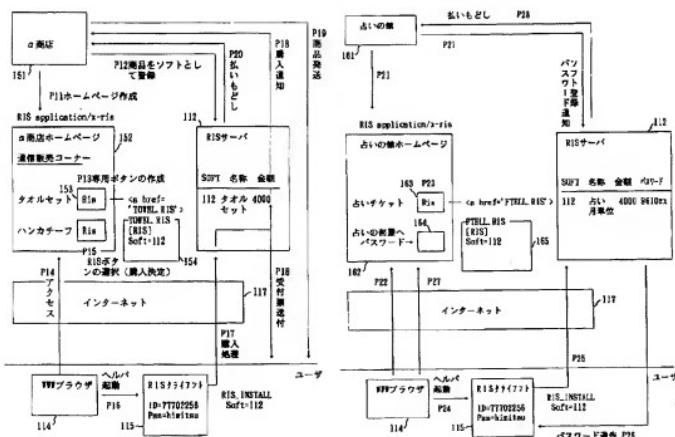
165



[图 1-4]

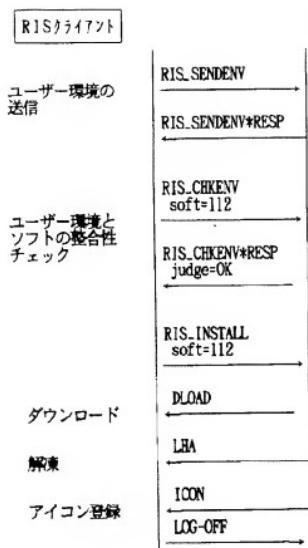
[圖 1-6]

オンラインショッピングシステムを示す図



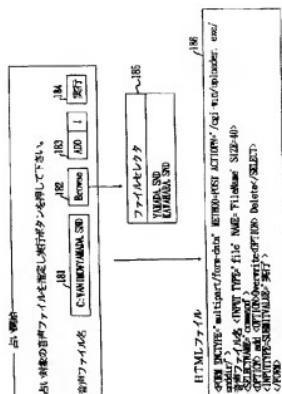
【図1-1】

ソフトウェアの配達を示す図



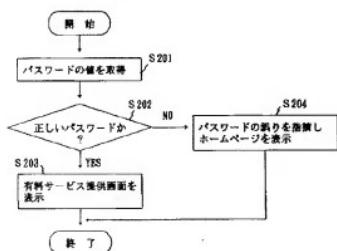
【图2.5】

古い開始画面を示す



【图20】

サービス利用権の確認処理のフローチャート URL格納ファイルを示す図



【图22】

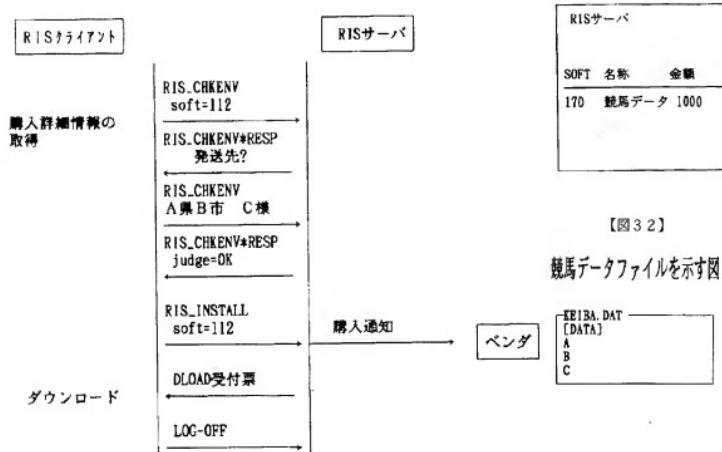
WORK URL
[URL]
URL=<http://www.ura.co.jp/ura.html>

[InternetShortcut]
URL=<http://www.ura.co.jp/ura.html>

*モザイクの場合

【図15】

受付票 / 購入通知送付処理を示す図 RISサーバの情報を示す図

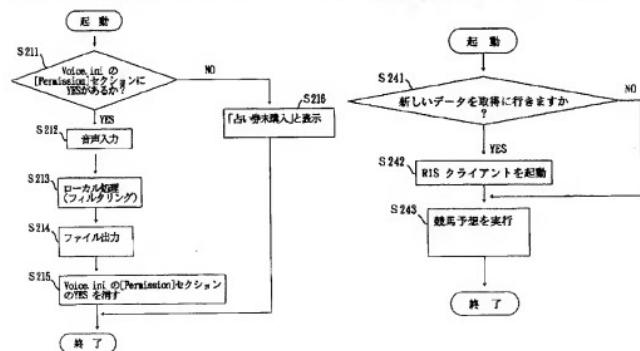


【図32】

競馬データファイルを示す図

【図24】

第1のVoice処理プログラムのフローチャート 第1の競馬予想処理のフローチャート



【図17】

占いの館ホームページのHTMLファイルを示す図　日付・ファイル名
対応表を示す図

```
<html>
<head>
<title> 占いの館HomePage</title>
</head>
<body>
~
<b>
占いチケット</b>
<a href='FTELL.RIS'>
<image src='ticket.JIF'></a>
<b>
占いの部屋へ</b>
<form method=GET action='http://www.ura.co.jp/ura.cgi'>
パスワード→<br>          <input name=password><br>
</form> <image src='infstell.JIF'></a>
~
</body>
</html>
```

96.4.1	FILE1.LZH
96.6.1	FILE2.LZH
96.8.1	FILE3.LZH

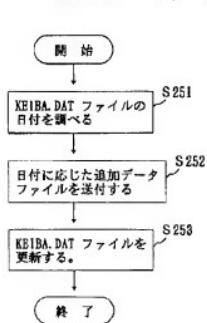
【図33】

【図31】

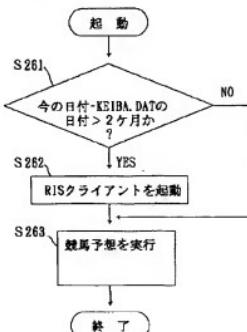
【図34】

【図35】

データのデストリビューション 各ファイルに含まれるデータを示す図 第2の競馬予想処理のフローチャート
処理のフローチャート

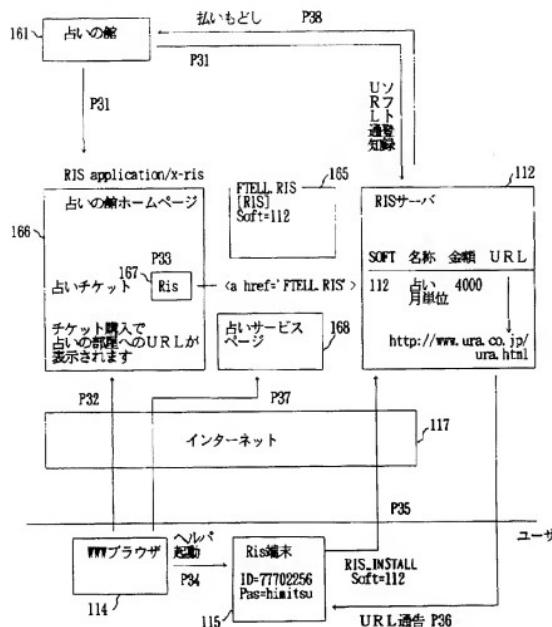


	D	E	F	G
FILE1.LZH	○	○	○	○
FILE2.LZH		○	○	○
FILE3.LZH			○	○



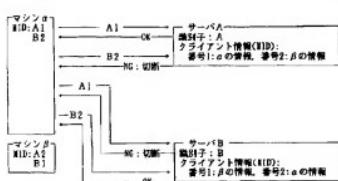
【図21】

URLを通知する通信サービスシステムを示す図



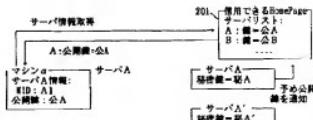
【図36】

複数のサーバが存在するシステムを示す図



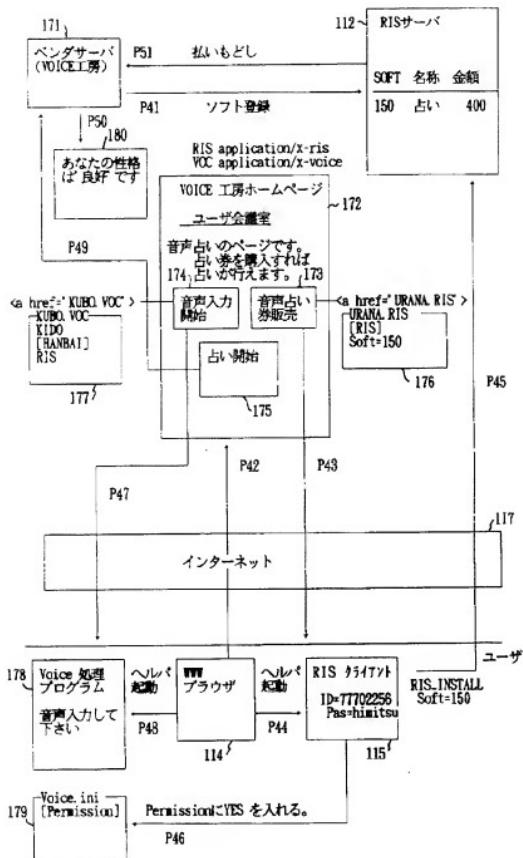
【図39】

サーバ接続システムを示す図



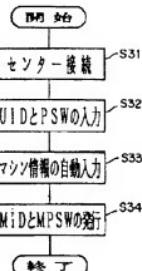
【図2.3】

第1のトランザクションサービスシステムを示す図



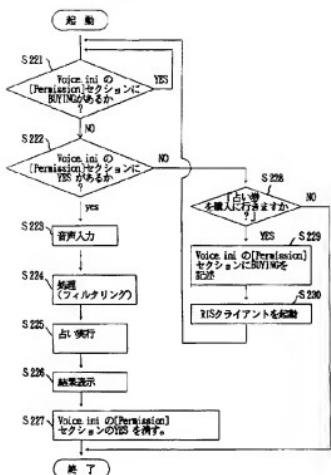
【図4.8】

端末ID登録のフローチャート



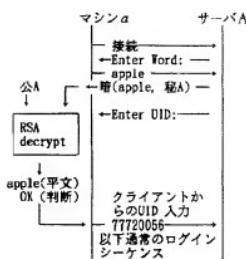
【図26】

トランザクション処理プログラムのフローチャート



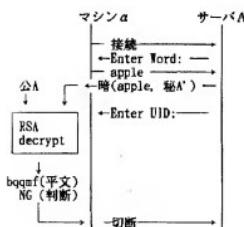
【図40】

第2のログインシーケンスを示す図



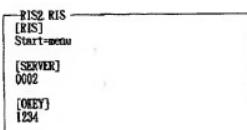
【図41】

第3のログインシーケンスを示す図



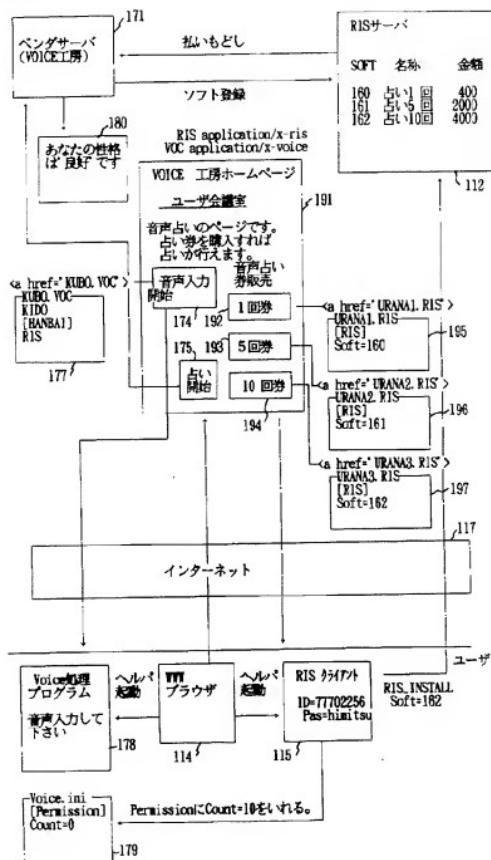
【図42】

第3のアンカーファイルを示す図



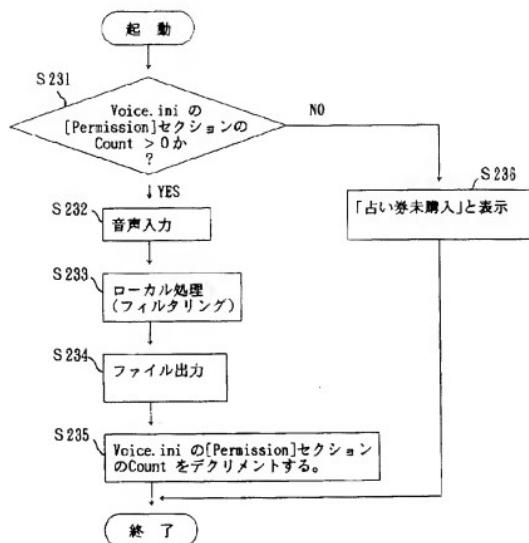
【図27】

第2のトランザクションサービスシステムを示す図



【図28】

第2のVoice処理プログラムのフローチャート



【図37】

第2の初期設定ファイルを示す図

```
RIS.INI
[SERVER]
0001
[INFO] :*****+
;SOUKODIR:金剛ケーブル
;WORKDIR:カーテンケーブル
;HOSTTEL:ホスト電話番号
;LSCRIPT:ホストオフ(カーテン)(標準端末と同じ文法)
;COMPORT:ComポートID
;
LSCRIPT=~\N[*]\C RIS~\N[COM]![Enter User-ID --->]\$ID/P36/V101~\N[Enter
Password:SPY~\N[Accepted/P38/V101]
COMPORT=3
RISDIR=C:\RIS\418RISWIN32
SOUKODIR=C:\RIS\418VSOURCE
WORKDIR=C:\RIS\418RISWORK
HOSTTEL=044-798-6500
INITFLAG=
[IDENT] :*****+
;UID :3-F ID
;PASSWD :A37-F
;
TELAREA=044
→ UID=77702256
→ PASSWD=BAGFDEOFMFOEOEAFNB
KEY=STFA40972F26A8A6B
[MACHINE] :*****+
;MODEL :ナカニシ
;OS :OS-2-F
;VID :マジックID
;NTRANID :マジックID
;
DS=2-
MODEL=3
VID=537
NTRANID=001087127712
;VID=41
;NTRANID=000091397010
;
[INET]
inetPermission=Yes
HOST=r1a.gemet.or.jp
PORT=5021
UsingINET=Yes
;
[EXTENSION]
RIS1.INI=ON
RIS2.INI=ON
RIS3.INI=OFF
```

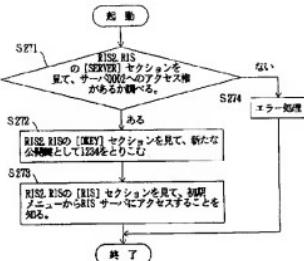
【図38】

第3の初期設定ファイルを示す図

```
RIS2.INI
[SERVER]
0002
[INFO] ;*****+
; SOUDODIR : 音楽ディレクトリ
; WORKDIR : ワークディレクトリ
; HOSTTEL : ホスト電話番号
; LSSCRIPT : イントロディクタ（標準端末と同じ文法）
; COMPORT : ComPort-ID
;
LSSCRIPT="M[*]C RIS2[COM!]![Enter User-ID --->]SID/P38/V10]"M[Enter
Password ->]P[PW][Accepted/P38/V10]"
COMPORT=3
RISDIR=C:\RIS\418\RIS\WIN32
SOUNDODIR=C:\RIS\418\SOUNDO
WORKDIR=C:\RIS\418\RIS\WORK
HOSTTEL=044-798-6501
INITFLAG=1
;
[IDENT] ;*****+
; UID : ユーザID
; PASSWD : パスワード
;
TELAREA=044
UID=11102256
→ PASSWD=BACFDDEOFNHOEDEAFNB
KEY=54FA40972F46A8A6B
;
[MACHINE] ;*****+
; MODEL : モデルコード
; OS : OSコード
; MID : マシンID
; MTRANID : マシントランクトID
;
OS=2
MODEL=3
MID=637
MTRANID=002087127712
[INET]
inetPermission=Yes
HOST=rис2.gmnet.or.jp
PORT=5021
UsingINET=Yes
```

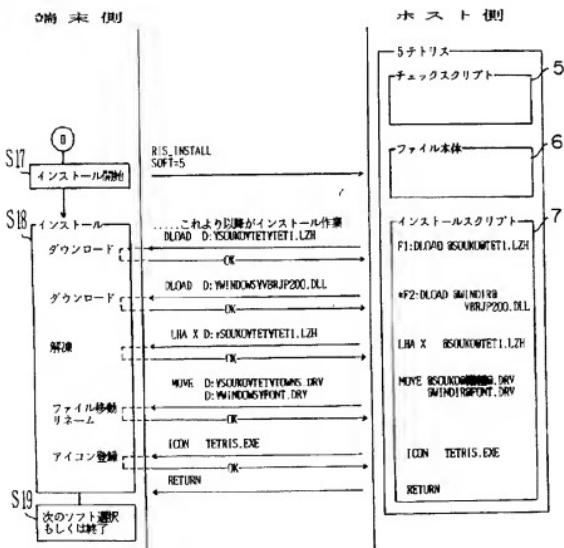
【図43】

クライアントの処理のフローチャート



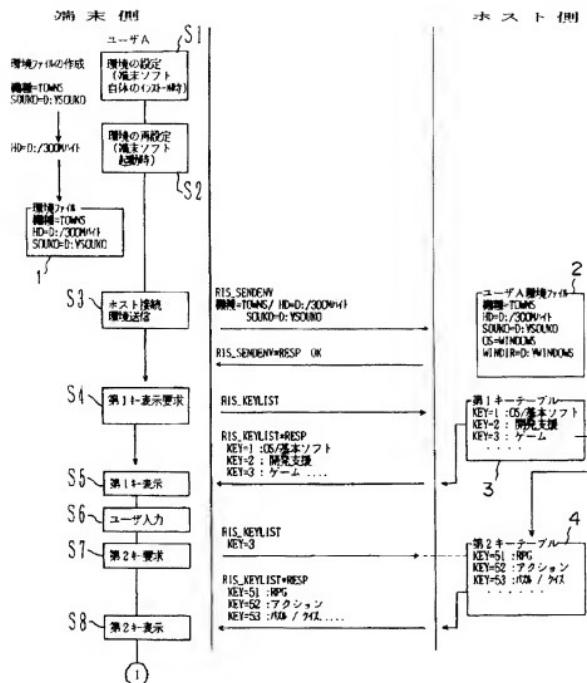
【図46】

リモートインストールのフローチャート(その3)



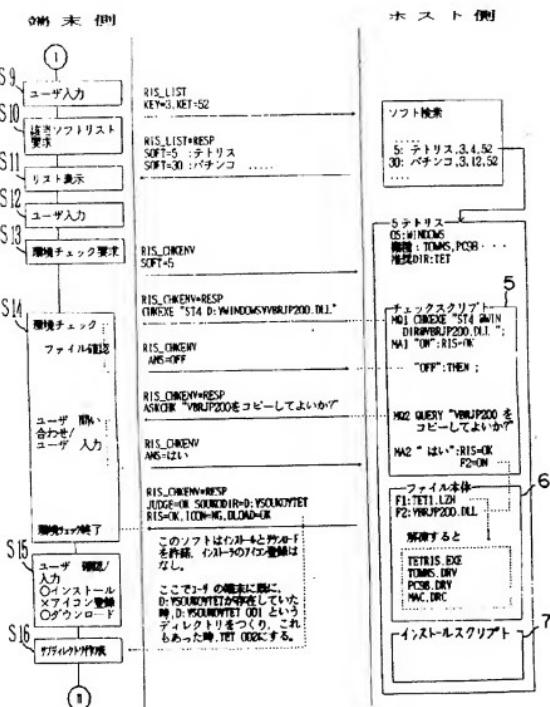
【図44】

リモートインストールのフローチャート(その1)



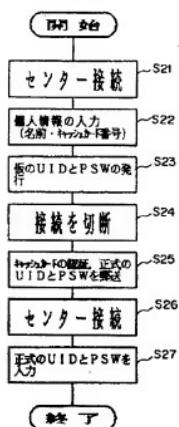
【図45】

リモートインストールのフローチャート(その2)



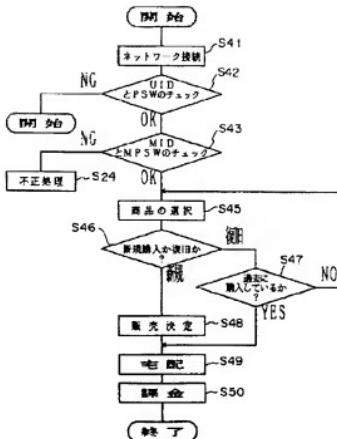
【図47】

ユーザID登録のフローチャート



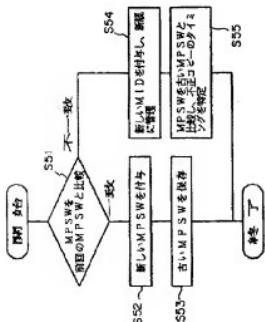
【図49】

販売のフローチャート



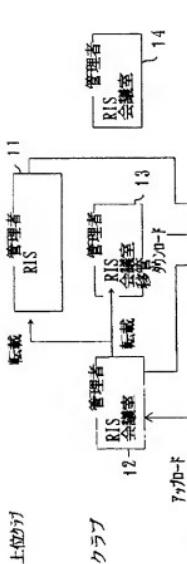
【図50】

端末パスワードチェックのフローチャート



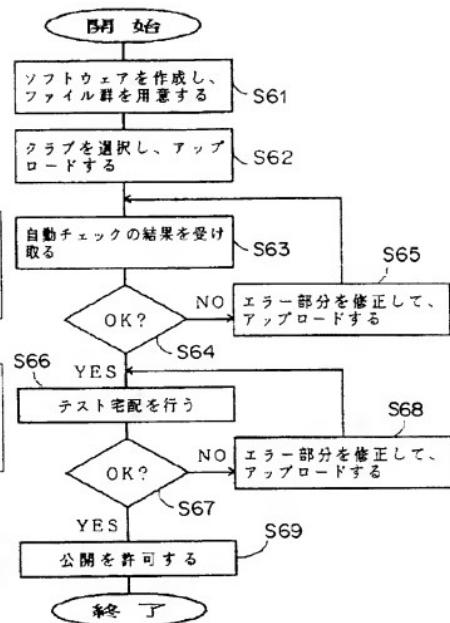
【図51】

場の構成を示す図



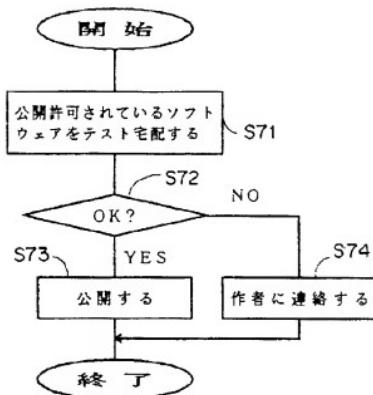
【図52】

作者の作業のフロー・チャート



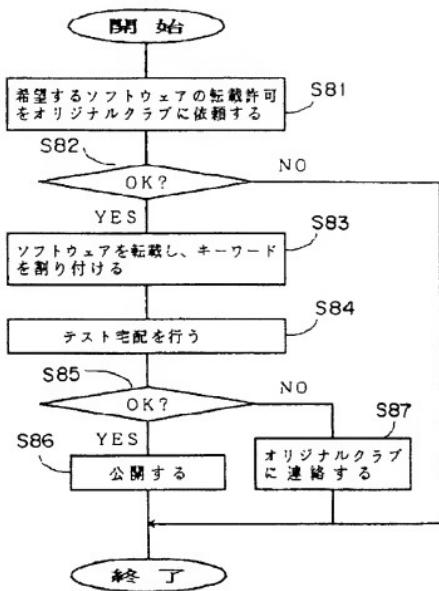
【図53】

オリジナルクラブ管理者の作業のフローチャート



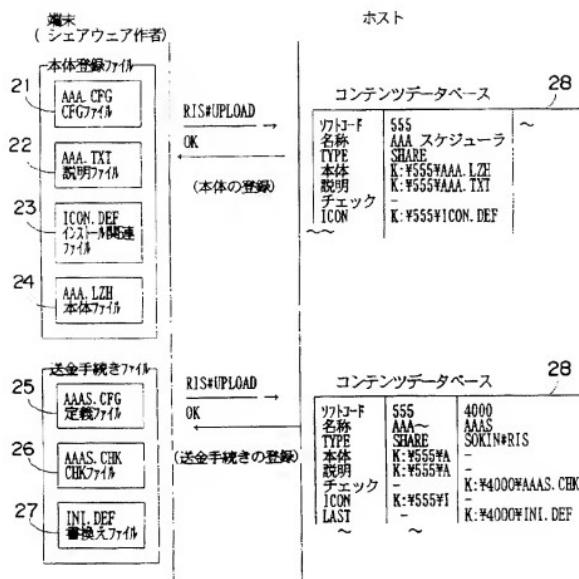
【図54】

転載先クラブ管理者の作業のフローチャート



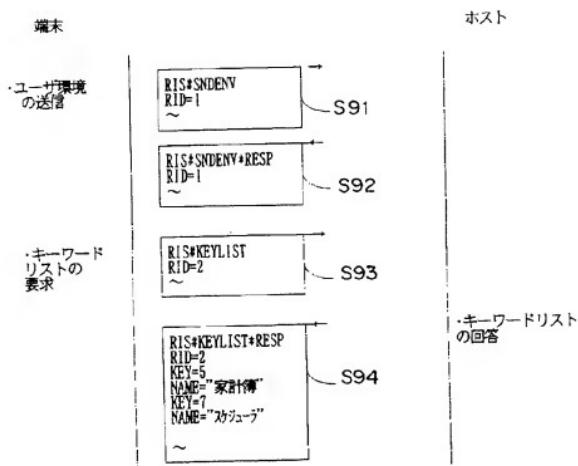
【図55】

アップロードを示す図



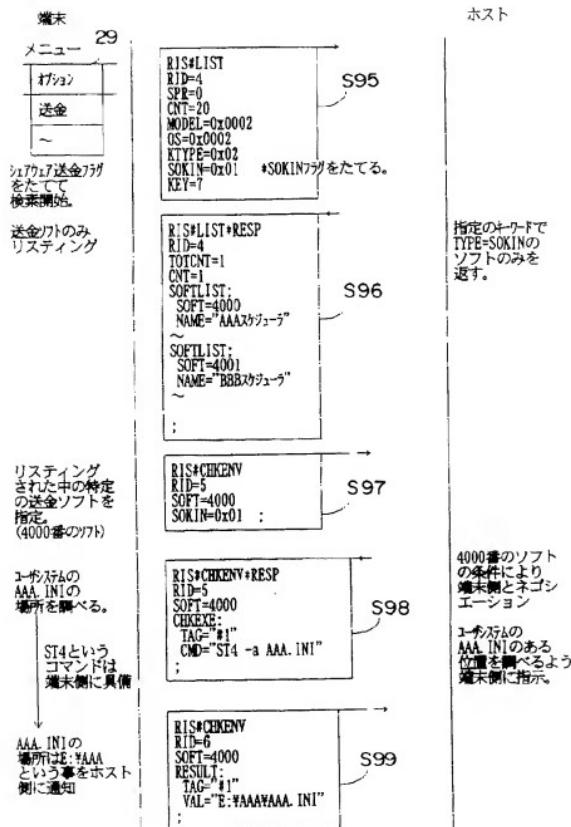
【図56】

シェアウェア手続きを示す図（その1）



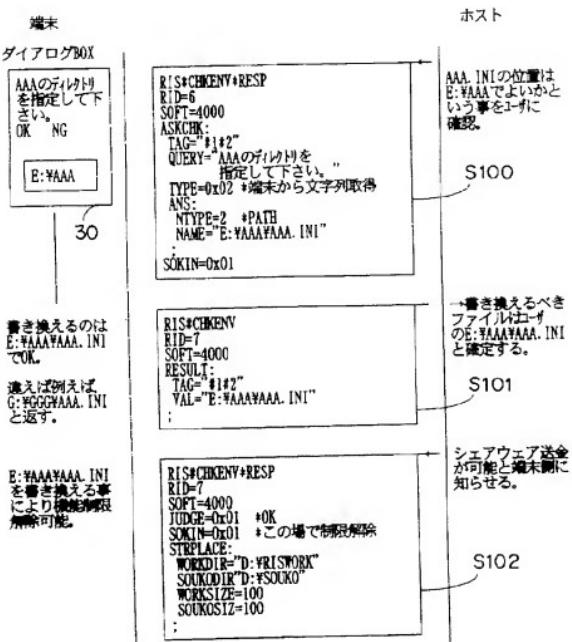
【図57】

シェアウェア手続書きを示す図（その2）



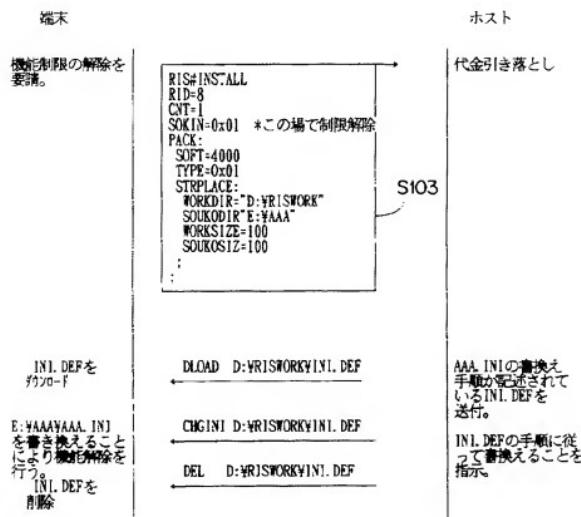
【図58】

シェアウェア手続きを示す図（その3）



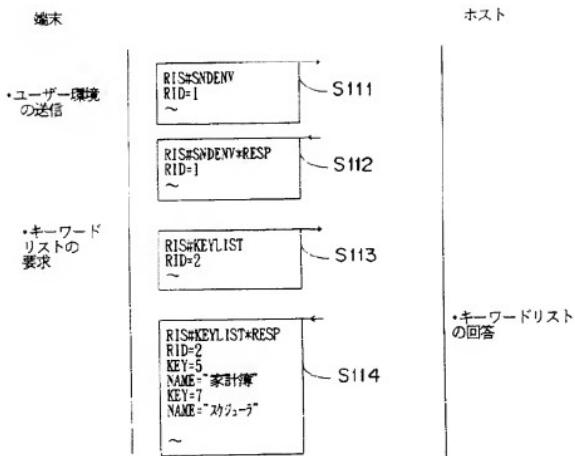
【図59】

シェアウェア手続きを示す図（その4）



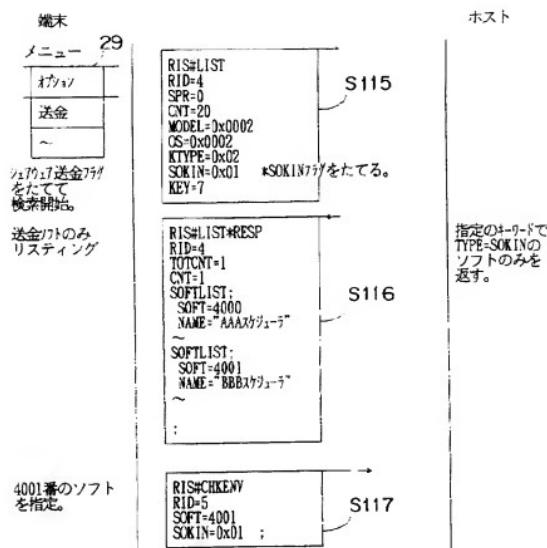
【図60】

代金弓き落とし手続きを示す図（その1）



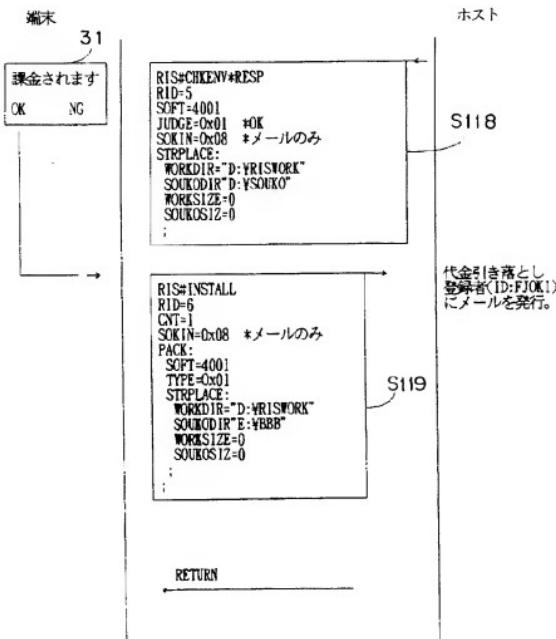
【図61】

代金引き落とし手続きを示す図（その2）



【図62】

代金引き落とし手続きを示す図（その3）



フロントページの続き

(72)発明者 中村 直人

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(72)発明者 山岸 利哉

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(72)発明者 関田 利司郎

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内